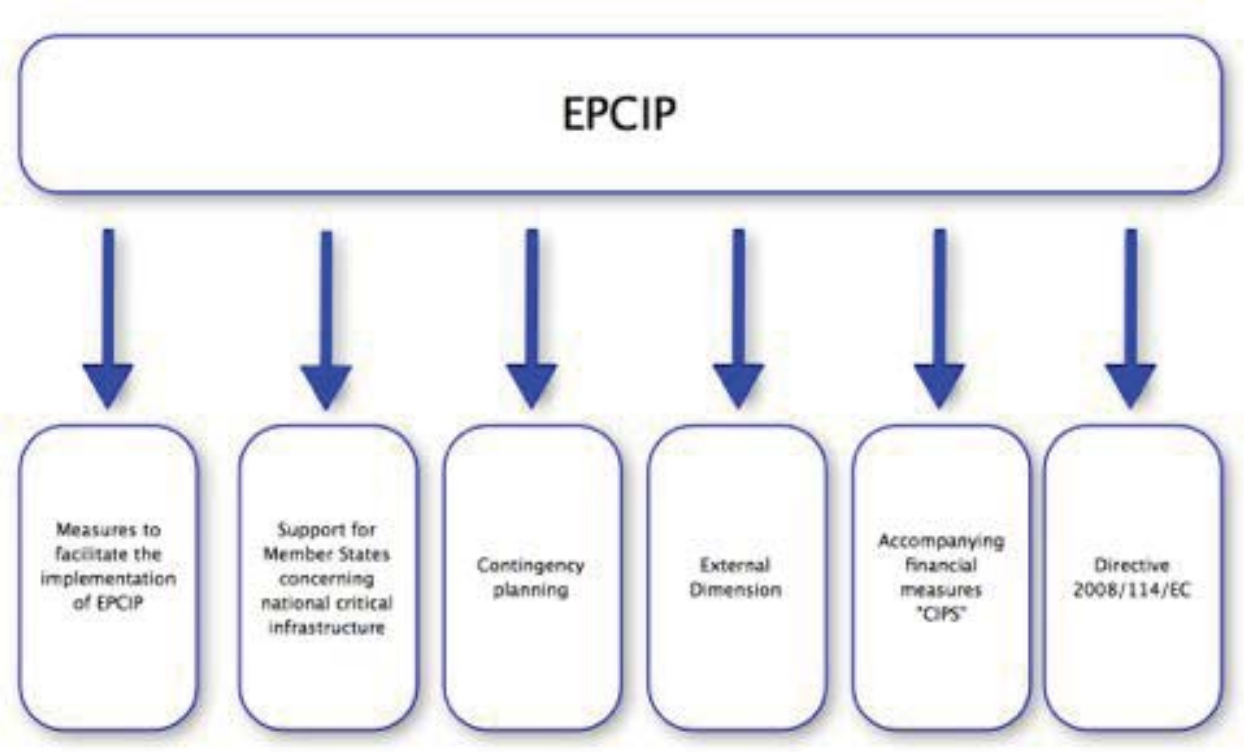
CIPS II workshop on research projects financed under the CIPS specific programme

Workshop Proceedings
22-23 November 2012
Ispra, Italy

Georgios Giannopoulos

2012



Report EUR 25747 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 210, 21027 Ispra (VA), Italy
E-mail: georgios.giannopoulos@jrc.ec.europa.eu
Tel.: +39 0332 78 6211
Fax: +39 0332 78 5469

http://stanet.jrc.it/
http://www.jrc.ec.europa.eu/

JRC 78267

EUR 25747 EN
ISBN 978-92-79-28183-9
ISSN 1831-9424

doi:10.2788/79113

Luxembourg: Publications Office of the European Union, 2013

Printed in Italy

Contents

CIPS II workshop on research projects financed under the CIPS specific programme

1 Background and purpose of the Workshop

The specific programme "Prevention, Preparedness and Consequence Management of Terrorism and Security related risks", part of the General Programme on Security and Safeguarding Liberties, provides financial support for operational cooperation and coordination actions (strengthening networking, mutual confidence and understanding, developing contingency plans, exchanging and disseminating information, experiences and best practices).

The programme activities cover both prevention and preparedness, particularly by improving the protection of critical infrastructures and consequence management to ensure the smooth coordination of crisis management and security actions, in particular regarding terrorist attacks. The budget for the CIPS funding scheme is 140 MEuro for the period 2007-2013. JRC activities supporting DG HOME in the implementation of the EPCIP are also financed by the CIPS funding scheme. JRC has a long history in supporting DG HOME and in organising similar events. The first CIPS conference was organised

in Rome in 2011, a series of Directive Implementation and Application workshops have taken place since 2009 as well as supporting events such as the Risk Assessment and Resilience workshop that took place in Ispra in April 2012. As a consequence JRC organised on the 22-23 of November the second workshop on CIPS funded projects.

The aim of this workshop is to bring closer research institutes that are financed by the CIPS scheme, national and European authorities and policy makers in order to exchange views on hot topics in the domain of research for critical infrastructures protection. In addition, it is an important event to demonstrate main achievements up to now for selected CIPS projects. The selected projects are financed by the CIPS Annual Work Programme (AWP) 2010 and 2011. These projects have usually a duration of 24 months (although certain projects are financed for shorter periods). Considering that projects financed by previous AWP were already presented in the first CIPS, it was clear that projects from 2010-2011 AWP should be presented in order to provide to the participants the latest developments in the domain of security research and Critical Infrastructures Protection.

The selection was based on the following criteria:

- Projects with a European dimension covering the maximum possible extent of operators and having an international dimension and significant impact to the EU in general
- Projects with an innovative concept
- Projects with strong potential for providing solutions to the end users
- Projects that address issues related to the upcoming EPCIP policy package and the main topics that have been discussed during the review process such as interdependencies, risk assessment and resilience.
- Projects with cross-sectoral dimension.

In general the projects that have been financed by AWP 2011 are still in a preliminary phase. For these projects this workshop was an opportunity to receive feedback in order to streamline research activities. Projects financed by AWP 2010 were in a more mature phase, thus more tangible results could be provided to the participants.

2 Future meetings

Taking into account the participants feedback such events are useful for both policy makers and researchers in order to improve the communication between these communities. In addition, the CIPS funding scheme provides an excellent opportunity to support projects that are tailored to the CIP domain and may provide innovative solutions for the policy makers. The intention is to continue organising these events on an annual basis. This will allow to obtain the latest developments in the domain of research and steer in a more efficient way ongoing projects towards achieving the high-level objectives of the EPCIP.

3 Annexes

- CIPS II Workshop agenda
- List of Participants
- Critical Infrastructure Simulation of Advanced Models on Interconnected Networks resilience
- Business Continuity Planning for Critical Infrastructures
- Security Risk Management Processes for Road Infrastructures

- Development Of a Risk Assessment methodology to Enhance security Awareness in ATM
- Critical ICT Infrastructures Simulation of Interdependency Model II
- Online identification of Failure and Attack on interdependent Critical Infrastructures
- Threat-Vulnerability Path Identification for Critical Infrastructures Compilation of a comprehensive all-hazards catalogue for critical infrastructure
- Risk Assessment and Development of Protection Capacity for Critical Infrastructures due to Aircraft Attack
- RAPID-N: A tool for mapping Natech risk due to earthquakes
- Development of a Risk Assessment and Resilience analysis platform by the JRC

CIPS II Workshop agenda

JRC Ispra, 22-23 November 2012

European Commission

JRC Sites

OUR MISSION

The mission of the Joint Research Centre is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of European Union policies. As a service of the European Commission, the Joint Research Centre functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

Joint Research Centre

The European Commission's in-house scientific service

European Commission
Joint Research Centre (JRC)
External Communication Unit

Brussels Tel.: +32 2 299 02 66
Fax: +32 2 299 63 22

Ispra Tel.: +39 0332 78 98 89
Fax: +39 0332 78 54 09

E-mail: jrc-info@ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation

www.jrc.ec.europa.eu

2nd CIPS Workshop

JRC Ispra, 22-23 November 2012

The CIPS projects are financed by DG HOME within the framework of the specific programme «Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks»

Joint Research Centre

2nd CIPS Workshop

22 November 2012

9:00 9:30	Registration and welcome to the JRC *G. Giannopoulos, Joint Research Centre*
9:30 10:15	Critical Infrastructure Simulation of Advanced Models on Interconnected Networks resilience *R. Onori, «Sapienza» University of Rome*
10:15 11:00	Business Continuity Planning for Critical Infrastructures *D. Mosquera Benitez, ISDEFE*
11:00	**Coffee Break**
11:15 12:00	Security Risk Management Processes for Road Infrastructures *H. Kammerer, ILF Consulting Engineers*
12:00	**Lunch**
13:30 14:15	Development Of a Risk Assessment methodology to Enhance security Awareness in ATM *P. Altieri, SESM*
14:15 15:00	Critical ICT Infrastructures Simulation of Interdependency Model – II *J. Vivero Millor, GMV*
15:00	**Coffee Break**
15:15 16:00	Online identification of Failure and Attack on interdependent Critical Infrastructures, *R. Setola, , Universita degli Studi Roma Tre*
16:00 16:45	Threat-Vulnerability Path Identification for Critical Infrastructures Compilation of a comprehensive all-hazards catalogue for critical infrastructure *P. Trucco, Politecnico di Millano*
19:00	**Dinner**

JRC Ispra

23 November 2012

9:00 9:45	Risk Assessment and Development of Protection Capacity for Critical Infrastructures due to Aircraft Attack *F. O. Henkel, Wölfel Beratende Ingenieure*
9:45 10:30	RAPID-N: A risk assessment tool for natural hazards and chemical critical infrastructure *E. Krausmann, S. Girgi* *Joint Research Centre*
10:30	**Coffee Break**
10:45 12:00	Development of a Risk Assessment and Resilience analysis platform by the JRC *G. Giannopoulos, B. Dorneanu, O. Jonkeren* *Joint Research Centre*
12:30	**Lunch**
14:00	End of Workshop

22-23 November 2012

All participants have to register through the following link until 10 of November:
https://jrc-meeting-registration.jrc.ec.europa.eu/

The meeting will be held in:
JRC – Ispra, Building 58c, Auditorium

Airports in Milan are:
Milano Malpensa and Milano Linate

Local transports:
Transport from and to these airports and from and to the agreed hotels will be organized by JRC.

Hotel rooms have been pre-booked in the area. Please register by November 13th to secure a hotel room.

For information on the content of the workshop please contact:
Mr. Georgios Giannopoulos
+39 0332 786211
Georgios.GIANNOPOULOS@jrc.ec.europa.eu

For organizational issues please contact:
Ms. Laurence Campé :
+39 0332 785032
Laurence.CAMPE@ec.europa.eu

List of participants

II CIPS Conference
Participants Details - 22/11/2012 to 23/11/2012

T O T A L P A R T I C I P A N T S: 40

ALTIERI PALMA
SESM Advanced solutions for Systems and Models
Via Circumvallazione Esterna
80014 GIUGLIANO IN CAMPANIA (Italy)
tel: +390818180395
fax: paltieri@sesm.it
E-mail: paltieri@sesm.it

ARMENIA STEFANO
CATTID - Università degli Studi di Roma "Sapienza"
Via Carlo Sereni 12
00146 ROMA (Italy)
tel: +393338711021
E-mail: armenia@cattid.uniroma1.it

BOOGAARD ROBERT
Schedeldoekshaven 200
2500 EZ THE HAGUE (Netherlands)
tel: 0031704266802
E-mail: r.r.boogaard@nctv.minvenj.nl

BREEDVELD MARIJE
Ministry of Security and Justice Netherlands
Schedeldoekshaven 200
2511EZ THE HAGUE (Netherlands)
tel: +31704266728
E-mail: m.h.breedveld@nctv.minvenj.nl

CALANDRI FABRIZIO
Istituto SITI
Via Pier Carlo Boggio 61
10138 TORINO (Italy)
tel: 3771220025
fax: 01119751122
E-mail: fabrizio.calandri@polito.it

CREMONA GEORGE
MALTA POLICE FORCE
POLICE GENERAL HEADQUARTERS
CRM1000 FLORIANA (Malta)
tel: +35622942101
fax: +35621255244
E-mail: george.a.cremona@gov.mt

DORNEANU BOGDAN
Joint Research Centre
Via Enrico Fermi 2749
21027 ISPRA (Italy)
tel: 00390332785156
fax: 00390332785469
E-mail: bogdan.dorneanu@jrc.ec.europa.eu

DR. GÖRÖG KATALIN
National DG for Disaster Management
Mogyoródi út 43.
1149 BUDAPEST (Hungary)
E-mail: katalin.gorog@katved.gov.hu

FIORE ENRICO
Istituto SITI
Via Pier Carlo Boggio 61
10138 TORINO (Italy)
tel: 3384155339

GATTINESI PETER
Stratiqo
Italy
E-mail: peter.gattinesi@ext.jrc.ec.europa

E-mail: enricofiore@siti.polito.it

GIANNOPOULOS GEORGIOS

European Commission - JRC - IHCP - Chemical Assessment and Testing Unit

Via E. Fermi 2749 - TP281

21027 ISPRA (Italy)

tel: +39 0332 786211

fax: +39 0332 789453

E-mail: georgios.giannopoulos@jrc.ec.europa.eu

GIRGIN SERKAN

tel: 3680

fax: 5469

E-mail: serkan.girgin@jrc.ec.europa.eu

GRUBER JAN

Ministry of Transport

nabrezi Ludvika Svobody 12

110 15 PRAGUE (Czech rep.)

tel: +420225131257

E-mail: jan.gruber@mdcr.cz

GRZYBOWSKI MICHAL

Government Centre for Security

Ujazdowskie 5

00 - 583 WARSAW (Poland)

tel: 0048222365899

fax: 0048222365898

E-mail: michal.grzybowski@rcb.gov.pl

HALLENCREUTZ-FOGTMANN EMMA

Danish Emergency Management Agency

Datavej 16

3460 BIRKERØD (Denmark)

tel: +4545906228

E-mail: ehc@brs.dk

HANZLÍKOVÁ HELENA

Ministry of Interior

Kloknerova 26

148 01 PRAHA (Czech rep.)

tel: 00420 950 819 875

fax: 00420 950 609

E-mail: helena.hanzlikova@grh.izscr.cz

HENKEL FRITZ-OTTO

Woelfel Beratende Ingenieure

Max-Planck-Str.

97204 HOECHBERG (Germany)

tel: +49-931-49708-310

fax: +49-931-49708-650

E-mail: henkel@woelfel.de

JONKEREN OLAF ERIK

Joint Research Centre

Via E. Fermi, 2749

I-21027 ISPRA (Italy)

E-mail: olaf.jonkeren@jrc.ec.europa.eu

KAMMERER HARALD
ILF Consulting Engineers
Harrachstrasse 26
4020 LINZ (Austria)

E-mail: Harald.Kammerer@ilf.com

KRAUSMANN ELISABETH
European Commission - Joint Research Centre
via Enrico Fermi 2749, TP361
21027 ISPRA (Italy)
tel: +39 0332 78 9612
fax: +39 0332 78 9007
E-mail: elisabeth.krausmann@jrc.it

LAZARI ALESSANDRO
Joint Research Centre
via enrico fermi
21027 ISPRA (Italy)

E-mail: alessandro.lazari@ext.jrc.ec.europa.eu

MARZI WILLI
Bundesministerium des Innern
Graurheindorfer Straße 198
53117 BONN (Germany)
tel: +49 228 99681 3778
fax: +49 228 99681 53778
E-mail: willi.marzi@bmi.bund.de

MOSQUERA DANIEL
ISDEFE
Beatriz de Bobadilla 3
28040 MADRID (Spain)

E-mail: dmosquera@isdefe.es

MRAČKA EDUARD
Ministry of Transport posts and Telecommunications
Nám slobody 6
81005 BRATISLAVA (Slovakia)

E-mail: eduard.mracka@telecom.gov.sk

NICOLAE MERLA
MAI - Centre for Coordination of CIP
Piata Revolutiei
010086 BUCHAREST (Romania)
tel: +40213140371

E-mail: merla.nicolae@mai.gov.ro

ONORI RICCARDO
CATTID - Università degli Studi di Roma "Sapienza"
Via Isole del Capo Verde, 45
00121 ROMA (Italy)
tel: +393288649469

E-mail: onori@cattid.uniroma1.it

PAIS SANTOS ISABEL
National Authority for Civil Protection
Estrada do Forte em Carnaxide
2794-112 CARNAXIDE (Portugal)
tel: + 351 21 424 71 00

E-mail: isabel.pais@prociv.pt

PALČIČ ROMEO
Ministry of Defence of the Republic of Slovenia
Vojkova cesta 55
1000 LJUBLJANA (Slovenia)

E-mail: romeo.palcic@mors.si

PETROVIC PETER
Ministry of Interior
Drienova 22
82604 BRATISLAVA (Slovakia)
tel: +421248593016
fax: +421248593344
E-mail: petrovic@uco.sk

PSCHIKAL ALEXANDER
Bundeskanzleramt
Ballhausplatz 2
1010 WIEN (Austria)
tel: 00431531152986
fax: 00431531152196
E-mail: alexander.pschikal@bka.gv.at

PURSIAINEN CHRISTER HENRIK

tel: 6032
fax: 5469
E-mail: christer.pursiainen@jrc.ec.europa.eu

RUSTHAUG CATO
Direc. for Civil Protection and Emergency Planning
Rambergveien 9
2014 TØNSBERG (Norway)

E-mail: cato.rusthaug@dsb.no

SCHIMMER MURIEL
Joint Research Centre
Via E. Fermi 1
I-21027 ISPRA (VA) (Italy)
tel: +390332785295

E-mail: muriel.schimmer@jrc.ec.europa.eu

SCHNEIDERS FRANZ-JOSEF
Federal Ministry of Transport
Robert-Schuman-Platz 1
53175 BONN (Germany)

E-mail: franz.schneiders@bmvbs.bund.de

SETOLA ROBERTO
University Campus Biomedico
Via A. Del Portillo 21
00128 ROME (Italy)
tel: +3906225419603
fax: +3906225419609
E-mail: r.setola@unicampus.it

SIEBER ALOIS

Via dei Ravasin 9b
21023 BESOZZO (Italy)
tel: int+39 0332 971374
fax: int+39 0332 971374
E-mail: alois.sieber@hotmail.com

THIBAULT ALEXANDRE
SGDSN
51 boulevard de la Tour-Maubourg
75007 PARIS (France)

E-mail: alexandre.thibault@sgdsn.gouv.fr

TRUCCO PAOLO
POLITECNICO DI MILANO
VIA LAMBRUSCHINI 4b
20156 MILAN (Italy)

E-mail: paolo.trucco@polimi.it

VESTRUCCI PAOLO
NIER Ingegneria SpA
Via Vincenzo Vela 8
40139 BOLOGNA (Italy)
tel: +390510391000
E-mail: p.vestrucci@niering.it

VIVERO JULIO
GMV
Isaac Newton, 11
28760 TRES CANTOS (Spain)
tel: +34918072100
fax: +34918072199
E-mail: jvivero@gmv.com

Critical Infrastructure Simulation of Advanced Models on Interconnected Networks resilience

Stefano Armenia

University of Rome "Sapienza"

email: armenia@cattid.uniroma1.it

CRISADMIN PROJECT

(HOME/2011/CIPS/AG/4000002116)

PROJECT SUMMARY

- **CRISADMIN** aims at developing a tool for the evaluation of the impacts of large catastrophic events and/or terroristic attacks on **Critical Infrastructures** (CIs).

- Such a tool will be designed as a decision support system with which to **experiment and analyze the interdependencies** among critical infrastructures, the modalities through which they get affected by predictable as well as unpredictable (or "black swan") catastrophic events (terroristic attacks, natural events, industrial disasters, etc.), as well as to investigate the risks and/or impacts of possible intervention countermeasures or prevention policies.

PROJECT OVERVIEW

Project name	**CR**itical **I**nfrastructure **S**imulation of **AD**vanced **M**odels on **I**nterconnected **N**etworks resilience - **CRISADMIN**
Action Grant	CIPS 2011 Action Grant (HOME/2011/CIPS/AG/4000002116-CRISADMIN)
Start and end date	01 September 2012 - 31 August 2014
Total budget	EUR 348,660.93
EU contribution	90%
Project Coordinator	**CATTID (Centre of Applications for Teleservices and Digital Technology innovation) - "Sapienza" University, Rome - Italy**
Project Partners	**Fondazione Formit**, Italy; **Theorematica Spa**, Italy; **Euro Works Consulting**, Belgium; **Erasmus Universiteit Rotterdam**, the Netherlands

PROJECT OBJECTIVES

- Provide decision makers with a tool to understand, evaluate and update already implemented processes and procedures for crisis management.
- For this purpose, the dynamic simulation model will consider the decision-making process under the conditions arising in a given observed scenario. Based on the perspective introduced by the SD methodology, the formulation of decisions is viewed as a continuous process of converting information into signals capable of feeding actions aimed at needed changes.
- Finally, after having identified the baseline for analysis, defined the logic circuits of cause and effect among key variables, and formulated a system dynamics model, a simulation environment (or DSS).

DURATION AND ROLES

- The project will have a total duration of 24 months, the kick-off date was September 7th, 2012;
- CATTID Sapienza will be responsible for the management of the project as well as for the development, testing and validation of the dynamic model, due to the expertise and research in the field of system dynamics;
- FORMIT will be responsible for the activity of data acquisition and data analysis concerning with the scenarios on which we will test the model and the possible strategies, as well as for the project dissemination;
- THEOREMATICA will be responsible for the development of the theoretical and analytical models underlying the various infrastructures and the relationships that drive the documented behaviours in the absence of a defined interconnection with other infrastructures and with the social system. Also, THEO will develop the software tool that will be used as a decision support system by the associate partners and the end-users who manifested their interest in contributing to the project;
- ROTTERDAM UNIVERSITY will provide its expertise in the field of the emergency management and communication in crisis situations, with particular reference to the experimentation with different policies and strategies on the DSS prototype;
- EU-WORKS will provide its expertise as technical support in the management and dissemination of EU projects.

ORGANISATIONAL STRUCTURE

KEY STAKEHOLDERS

- All the R&D activities planned by the consortium will be furthermore enhanced by the involvement of field experts (in the fields of System Dynamics, of Critical Infrastructure Protection and of Terrorism Countermeasures) through an **Expert Advisory Board** (**EAB**), that will support all the project phases, from the definition of requirements to the model construction to the final validation of the DSS prototype, as well as through the involvement of end-users (organized in an **end-user committee** – **EUC**).

- There will be two categories of users:
  - users who join the project (also at later stages) as **Associate Partners**, that are official project partners (but non co-beneficiaries of any grant) who will be allowed to freely use and experiment with the DSS prototype
  - users who will manifest their interest in the project in a lighter way (by signing this letter of manifestation of interest), that will have the chance to provide data and information and will receive back from the project the main results as well as a visibility at the project level (they will be included in the EUC)

PROJECT OBJECTIVES /1

The final goals of CRISADMIN are:

- to develop a model that will be included in a **decision support system prototype** which will be useful for the assessment and management of critical events, and in particular for the simulation and development of both preventive measures and response activities during the emergency.

- due to the development of methods, techniques and instruments for operational and training use (in order to increase the security awareness of critical infrastructures operators), the project will allow for an **exchange and dissemination of information, experience and best practices** between Member States and between the different organizations/bodies responsible for the protection of critical infrastructures, also by creating an informal contact networks between authorities.

PROJECT OBJECTIVES /2

- The simulation model will be made available under the form of prototype decision tool to institutions and organizations, both public - civil protection, fire brigades, etc. - and private (individual IC) throughout the EU Member States.

- End-users (institutions or organizations) will have the chance to freely use the prototype and experiment with it so that, after testing and assessing its validity, they will also be put in the conditions to customize it, based on their specific needs.

STATE OF THE ART

- Several research and policy studies have been conducted to develop methods to improve protection of Critical Infrastructures, and to analyze their behavior both from an economical and social point of view.

- Utilities, and other organisations who operate a country's critical infrastructure (CI), historically have a high level of competence concerning the assessment and mitigation of threats to the security and integrity of infrastructure they manage. They also have well established and tested procedures for recovering the infrastructure in the aftermath of a disruptive event.

- However in recent years new threats have emerged and the probability of known threats occurring has increased. As a result, traditional approaches to risk assessment and recovery planning have started to be questioned as to their continued relevance and fitness for purpose.

- Thus, better understanding is needed of the relationship between operational, commercial and regulatory pressures, the strategic choices these lead to on the part of infrastructure operators and the long-run consequences for the resilience of these systems and hence for service continuity.

- As might be expected, the issue of threat, risk and resilience of the utilities that make up the CIs has become a topic of considerable interest and concern since the terror attack of 9/11 and the evidence of more frequent and serious natural events.

- A multitude of groups, from widely diverse disciplines have applied a bewildering array of methods to study the issue.

Modelling risk & Resilience in utilities

- **A comprehensive, though now somewhat dated survey (given the rapid developments in modelling) was carried out by the Idaho National Laboratory in 2006.**
- Agent-based and network modelling methods are widely deployed, often in considerable detail and including geospatial data about network assets, in an effort to capture accurately the response of particular infrastructure networks.
- Many such models are intended for developing organisational readiness to respond to events, and for training, often by means of war-gaming exercises.
- Models range from detailed attention to occurrences and responses of individual assets up to whole-system models for an entire infrastructure system (power, telecommunications and so on). Some go so far as to capture the interactions between different infrastructure networks.
- In recent times, these researches began to employ the System Dynamics approach, even though it appears not to have been used extensively for modelling the dynamics of infrastructure risk, resilience and response, possibly because of the perceived need to deal with geospatial aspects of the problem (the proximity of assets to each other and to residential and commercial neighbourhoods) and the mechanical behaviours of physical assets

System Dynamics Advantages

- Although existing simulations for modelling risk and resilience are powerful and highly- developed, the present work is motivated by two perceived shortcomings.
  - **First**, few models appear to address the long-term strategic choices leading to a network's resilience and speed of recovery.
  - **Secondly**, most models are extremely large, detailed and complex, requiring considerable expertise and experience from their users.
- Some work has been done on the use of system control design to assess infrastructure resilience, but system dynamics offers additional advantages on these two issues.

What is System Dynamics

- Computer simulation modeling methodology for studying and managing complex feedback systems, such as business and other social systems
- System:
  - In general, a collection of interacting elements that function together for some purpose
  - Here, **feedback** is the differentiating descriptor
- Properties of dynamic problems:
  - Contain quantities that vary over time
  - Variability can be described causally
  - Important causal influences can be contained within a closed system of feedback loops

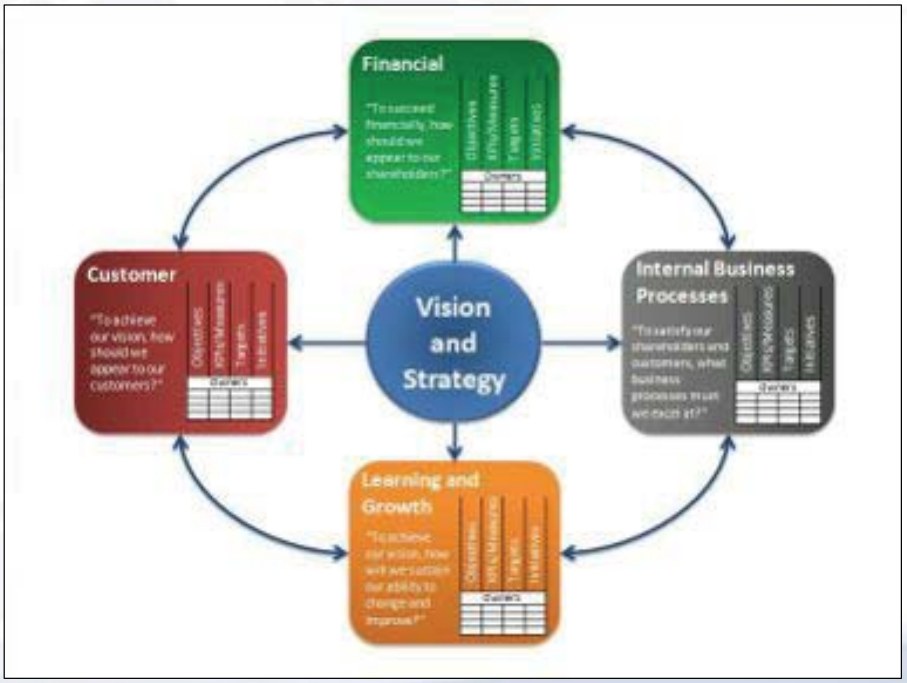
Applications of System Dynamics

- System Dynamics, as a decision-making modeling approach, is easily used in contexts where standard analysis is made difficult by the wide range of available data, especially in those systems highly influenced by the so called “soft” variables, those variables, usually connected to human behavior, that are not directly measurable (i.e. Customer Satisfaction, Panic Level, and so on).

- An example of analysis tool that highly benefits from the System Dynamics approach, due to the high interconnectedness of systems and variables within each system, is the Balanced Scorecard tool.

- In the Balanced Scorecard method, both soft and hard variables are measured and confronted at each step of the process, to monitor the causal loops between actions and the system’s responses.

The Balanced Scorecard Paradygm



US Dept. of Homeland Security – CIP/DSS

- Under current and future cyber and physical threat environment, the United States in 2003 decided to undergo a comprehensive approach to security for its critical infrastructure using vulnerability, consequence, and risk analyses.

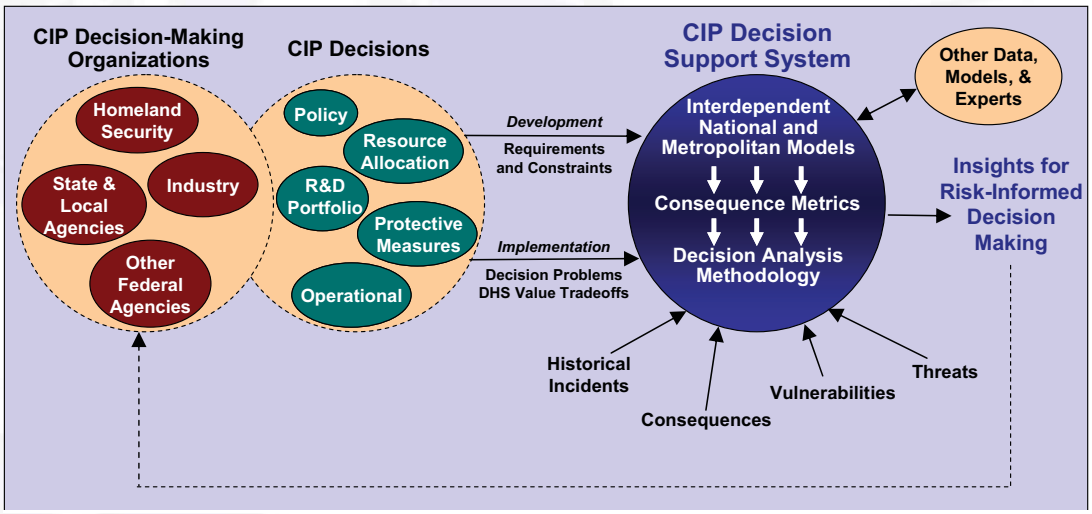
- The approach had to address uncertain and evolving threats, consider a wide variety of assets and infrastructures, and use consistent methodologies and criteria.

- The Critical Infrastructure Protection (CIP) Program sponsored by the U.S. Department of Homeland Security (DHS) had three primary goals:
  - Develop, implement, and evolve a rational approach for prioritizing CIP strategies and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks;
  - Propose and evaluate protection, mitigation, response, and recovery strategies and options; and
  - Provide real-time support to decision makers during crises and emergencies.

US Dept. of Homeland Security – CIP/DSS

- Decision makers need to understand the consequences of policy and investment options before they enact solutions, particularly for the highly complex alternatives available for protecting the nation's critical infrastructures in today's threat environment.
- The most effective way to examine tradeoffs between the benefits of risk reduction and the costs of protective action is to utilize a decision support system (DSS) that incorporates threat information, vulnerability assessments, and disruption consequences in quantitative analyses through advanced modeling and simulation.
- Government and industry decision makers can use such a DSS to prioritize protection, mitigation, response, and recovery strategies as well as to support red-team exercises and provide support during crises and emergencies.
- A system dynamics modeling, simulation, and analysis approach was used to conduct consequence assessments and risk analyses (based on realistic threats, system/infrastructure vulnerabilities for the threats, and resulting consequences).

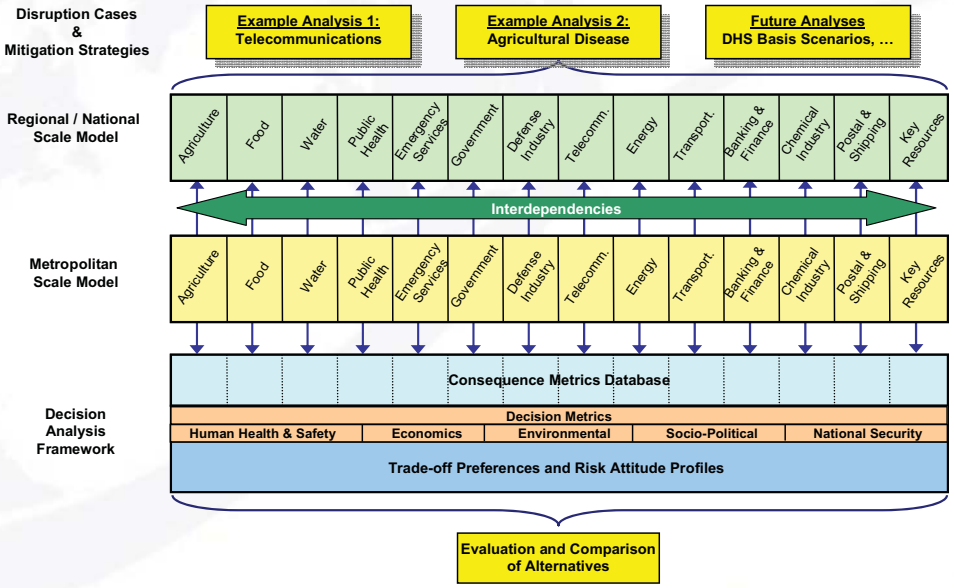
US Dept. of Homeland Security – CIP/DSS



Relationship between CIP decision makers, decisions, and the CIP/DSS.

Source: Bush et al. (2005)

US DEPT. OF HOMELAND SECURITY – CIP/DSS



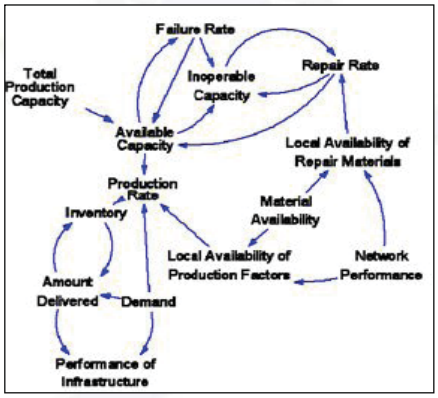
CIP/DSS architecture

Source: Bush et al. (2005)

US DEPT. OF HOMELAND SECURITY – CIP/DSS

- The consequence models simulate the dynamics of individual infrastructures and couple separate infrastructures to each other according to their interdependencies.
  - For example, repairing damage to the electric power grid in a city requires transportation to repair sites and delivery of parts, fuel for repair vehicles, telecommunications for problem diagnosis and coordination of repairs, and the availability of labor.
  - The repair itself involves diagnosis, ordering parts, dispatching crews, and performing repairs.
  - The electric power grid responds to the initial damage and to the completion of repairs with changes in its operating capacity (the number of megawatts that can be distributed to customers).
- Dynamic processes like these are represented in the CIP/DSS infrastructure sector simulations by differential equations, discrete events, and codified rules of operation.
- The following slide outlines the influences that generally are implemented in the critical infrastructure models.

SYSTEM DYNAMICS IN CI MANAGEMENT

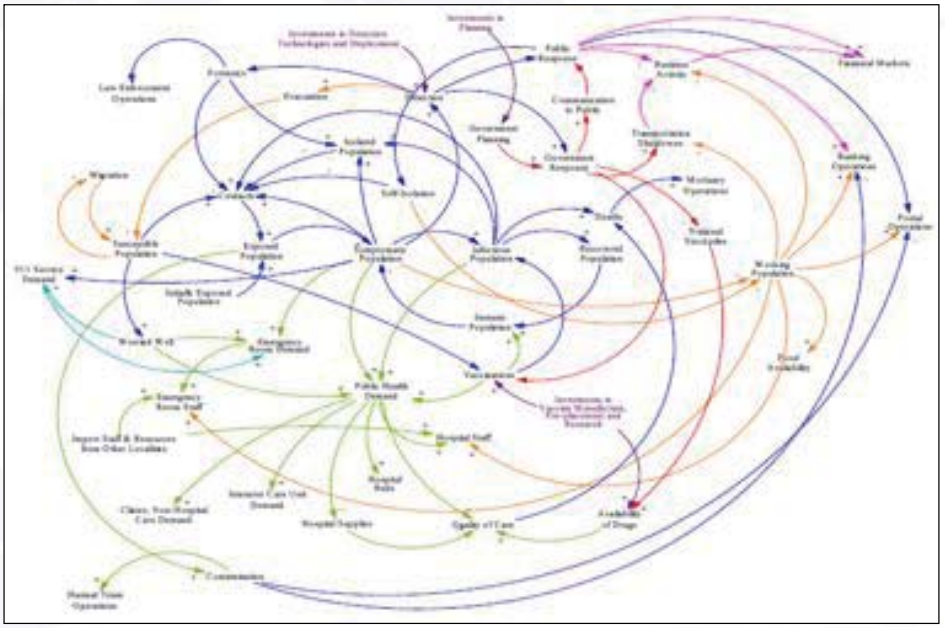


Generic influences in CIP/DSS critical infrastructure models.

Source: Bush et al. (2007)

When applied to the Critical Infrastructure management, the System Dynamics approach allows to consider every component of the causal relations and loops between e.g.: the public's behavior, the level of availability of the CI and the public's safety.

SYSTEM DYNAMICS IN CI MANAGEMENT



Influence diagram for cascading effects of infectious disease through critical infrastructures.

Source: Bush et al. (2007)

STATE OF THE ART

- "Modeling Economic Impacts to Critical Infrastructures in a System Dynamics Framework", Dauelsberg and Outkin (2005)

- Studies on the consequences of infrastructure disruptions from an economic point of view, leaving room for development on the "softer" aspects of the system behavior.

- In their approach they considered a disruption as an event that "topples" the equilibrium of the system; such a definition can be certainly applied to such an event as a natural or man/made disaster.

MODELING DISRUPTION IMPACTS

- Modeling economic impacts arising from disruptions to critical infrastructures is increasingly important for determining the most effective investment strategies for protective measures and loss mitigation if a disruption event occurs.

- While many mitigation measures may appear important and potentially cost-effective under certain circumstances, most government agencies need to rank these alternatives to effectively allocate their limited budgets.

- To rank these preventative measures, the economic costs and potential savings (reductions in lives lost or economic activity losses) need to be evaluated.

- It is also necessary to understand costs for the entire economy—beyond those of the initially impacted infrastructures—to fully comprehend the magnitude of the event and to make the appropriate allocation decisions.

Dynamic Nature of Disruption

- The economic impacts modeled in a system dynamics framework are built upon a collection of individual models of interdependent critical infrastructures (sectors).
- Dynamics of a sector are a function of the operations in that sector as well as operations in other infrastructures.
- The overall model uses these interactions and additional information to estimate total direct economic impacts from an incident.
- Such an approach allows us to estimate impacts to the economy represented as a dynamic system without requiring the assumptions of equilibrium solutions. In fact, economic impacts arising from disruptive events are perhaps better described as effects caused by disequilibrium dynamics.

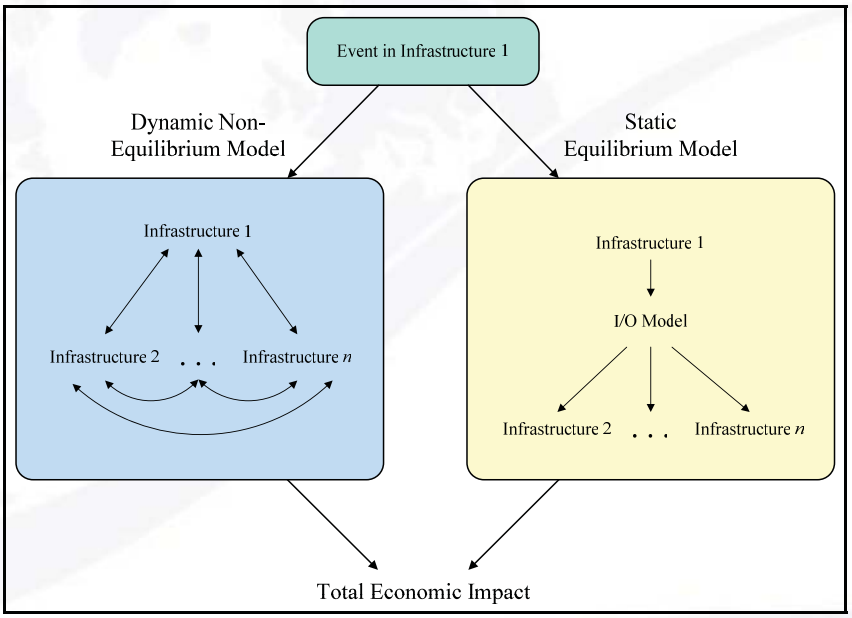
Methodological Approach

- Model the disruptions as they occur and propagate through the infrastructures.
- There are a number of interdependencies between infrastructures.
  - *For example, the banking and finance sector performance depends on the availability of telecommunications, energy, and labor force; emergency response depends upon roads, transportation, and telecommunications availability; food availability depends on agriculture and energy as well as other sectors; etc.*
- Therefore, even if a system was in equilibrium at the beginning of a scenario, because of the initial disruption and interactions between different sectors, we do not expect that the system will go through a set of equilibrium states during a scenario.
- Thus the goal is to **investigate and understand the non-equilibrium, non-linear dynamics of the system**.

SD MODELS VS. I/O MODELS

- A system dynamics (SD) model with multiple feedback structures is well suited for such a task.
- This is a point of departure from the input-output (I/O) approaches where equilibrium conditions are implied.
- However, during a disruptive event there are no apparent reasons why the equilibrium, as it is normally defined in economics, should occur.
- In general the incidents that are modeled by this system are transient in nature, often lasting no longer than a few weeks. I/O models are most often calibrated to annual data and intend to capture permanent changes and long term trends, smoothing out short term dynamics.

SD MODELS VS. I/O MODELS



Event Propagation in Dynamic Systems vs. I/O Model

Source: Dauelsberg, Outkin (2005)

Dynamic Vs. Static Models

- The dynamic nature of this approach allows to model the impacts as they occur in individual infrastructures.
- For example, if an event were to occur initially in one infrastructure, an SD model would simulate the impact to that infrastructure and its effect on other infrastructures in the system.
- Additionally, those secondarily affected infrastructures would **further propagate** the effects into other infrastructures as well as back into the initially affected infrastructure through feedback loops present in the system.
- On the other hand, generally, a static equilibrium model, such as an I/O model employs externally calculated primary economic effects to estimate total economic impacts by using I/O multipliers.

The Interconnection with the Social System

- An additional non-equilibrium component of such an approach is the ability to explicitly model the population's response to events.
- Model behaviors such as hording and latent demand: these behaviors are non-equilibrium in nature and may not be suitable for modeling in equilibrium-based tools.
- To estimate the economic effects, explicitly acknowledge that the state of the infrastructure within a certain area affects commerce and production within that area.
- Some of the main factors affecting commerce and production are: energy and telecommunications availability, transportation, labor force, etc.
- All of these are factors of production, contributing to either capital or labor components required for production or commerce to transpire.

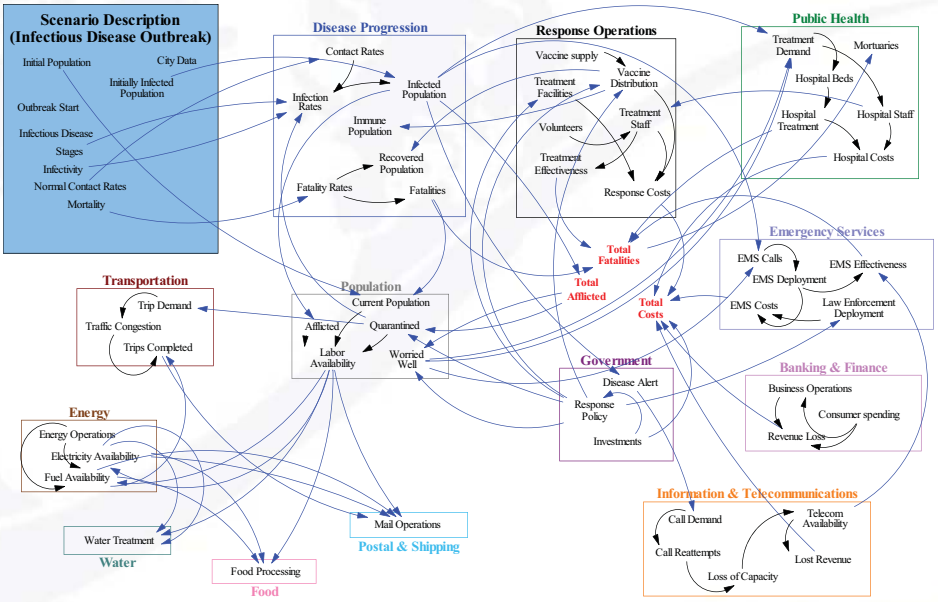
Critical Infrastructure Interdependency Example

- The CIP/DSS Metropolitan Model is a set of critical infrastructure subsectors modeled in a system dynamics framework using Vensim.
- The goal of the Metropolitan Model is to represent the interdependencies between infrastructures and simulate the disturbances that can start in one infrastructure and propagate to others.
- Every infrastructure—also called a sector—consists of a set of subsectors that represent the major portions of that sector. For example, the electricity subsector—a component of the Energy sector— models the generation, distribution, and consumption of electricity.
- Each sector models the broad capabilities of the infrastructure and is not intended to be a stand-alone, detailed model. Instead its strengths lie in the representation of **first order** interactions between sectors and the ability to model/show how a simple disruption in one sector can propagate to others and disrupt the entire system of critical infrastructures.

Critical Infrastructure Interdependency Example

- The following Causal Loop Diagram (CLD) represents the interdependencies in the infrastructure model from a scenario involving the release of an infectious disease.
- Effects spread through the population not only from initially and secondarily infected people, but through self and mandatory quarantine.
- Effects also spread into other sectors as less people use transportation to get to work and to shop.
- Public Health and Emergency Services experience increased demand as people seek medical treatment for the disease. Similar effects can be observed in other scenarios as one event spreads through many different sectors.

System Dynamics in CI management



Influence diagram for cascading effects of infectious disease through critical infrastructures.

Source: Dauelsberg, Outkin (2005)

State of the Art

- "When to use qualitative or quantitative system dynamics techniques: guidelines derived from analysis of recent man-made catastrophes", Mc Lucas

- Strong evidence towards the fact that System Dynamics allows to take into consideration the many complex variables that come into play in the decision-making stage of the managing of man-made catastrophes.

State of the Art

- "Understanding and Managing the Threat of Disruptive Events to the Critical National Infrastructure", Warren and Thurlby (2012)

- They further pointed out that System Dynamics can create tools that are both simpler and more accurate than those used to date in the managing of disruptive events to Critical Infrastructures, specifically in the decision-making support field.

State of the Art

- Many powerful simulation tools already exist to understand how networks could be affected physically by major incidents. Others , help organisations develop the readiness to respond to such incidents, often by war-gaming approaches.

- The part of the problem that is less well understood is the relationship between long-term, strategic choices and the ability of infrastructure networks to withstand disruptive events. Those choices concern investment in the assets themselves, in the IT infrastructure, especially the network control systems, and in the people managing the system.

- Whilst it is clear enough that "spending less on assets, systems and people will degrade the system", it is not so obvious how much impact any particular choice will have over long periods of time, nor how choices on different issues will interact.

- The issues that need to be better understood are therefore:
  - how long-term choices on strategic issues make the network more resilient (less likely to be damaged by a disruptive event)
  - how these and other choices can minimise the service loss when disruptive events do occur
  - how strategic and operational choices can minimise the time for the network to recover, and thus the total cumulative loss of service

The changing nature of Threats

- Until recently, the nature of disruptive threats to any part of the CIs was well understood.
- Infrastructure was designed to be able to resist the events to a certain point and then behave in such a way that failure was orderly and somewhat controllable, so that recovery after the event would be efficient.
- As a result, the failure of infrastructure components under normal operating conditions was rare. Disruptive events such as storms, human intervention and error were equally rare, and emergency procedures could minimise the effect of these and accelerate recovery.
- This resilience, though, came at a high cost, as the wider external environment started to change

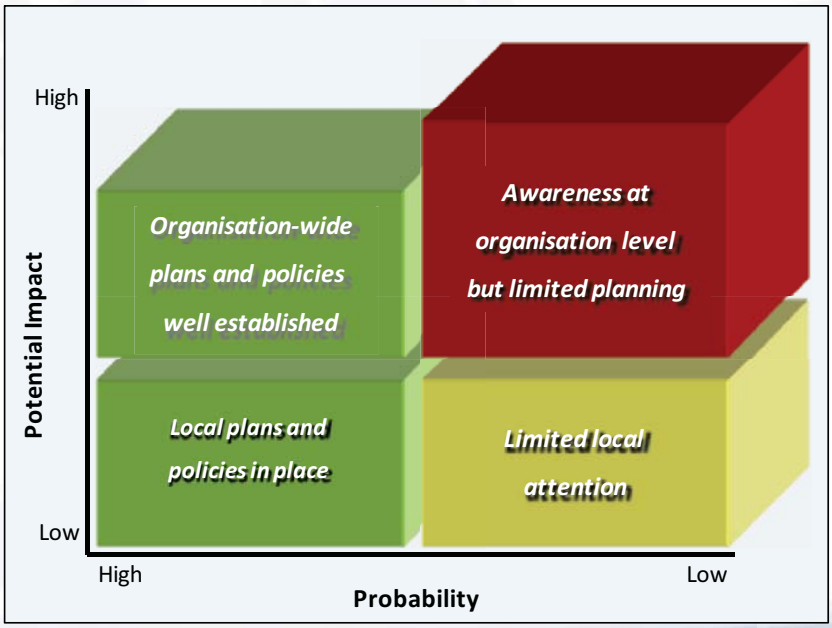
The changing nature of Threats

- Privatisation -> Asset "time bomb", by reducing maintenance and delaying replacement programmes (the concept of "asset" includes Human Resources…)
- Privatisation also shortened the time-horizon for both financial and regulatory objectives (short term vs long term asset lifecycle)
- Climate Change caused weather patterns to become both more erratic and more extreme.
- A new threat of terrorism and in particular cyber-terrorism also emerged (control-system damages)
- Lastly, as the CIs have become more sophisticated and more complex, their various parts have become more dependent on each other: this increased the risk of an event spreading across different parts of the CIs.

HIGH IMPACT – LOW PROBABILITY (BLACK SWAN)

- Attention has thus focused on high probability, high impact threats that are somewhat obvious.
- This strategy is, though, no longer adequate. Known threats have migrated towards the high impact, high probability quadrant and new threats have emerged, particularly in the low probability, high impact quadrant
- What is more, the possible consequences from these increasingly unpredictable risks can be much more severe and widespread than the more obvious examples for which contingencies already exist.
- The existing approach to risk assessment is no longer adequate for the more dynamic environment in which the CNI exists, especially as it is now older and more vulnerable to age- related threats.

HIGH IMPACT – LOW PROBABILITY (BLACK SWAN)



Resilience as a strategy/policy issue

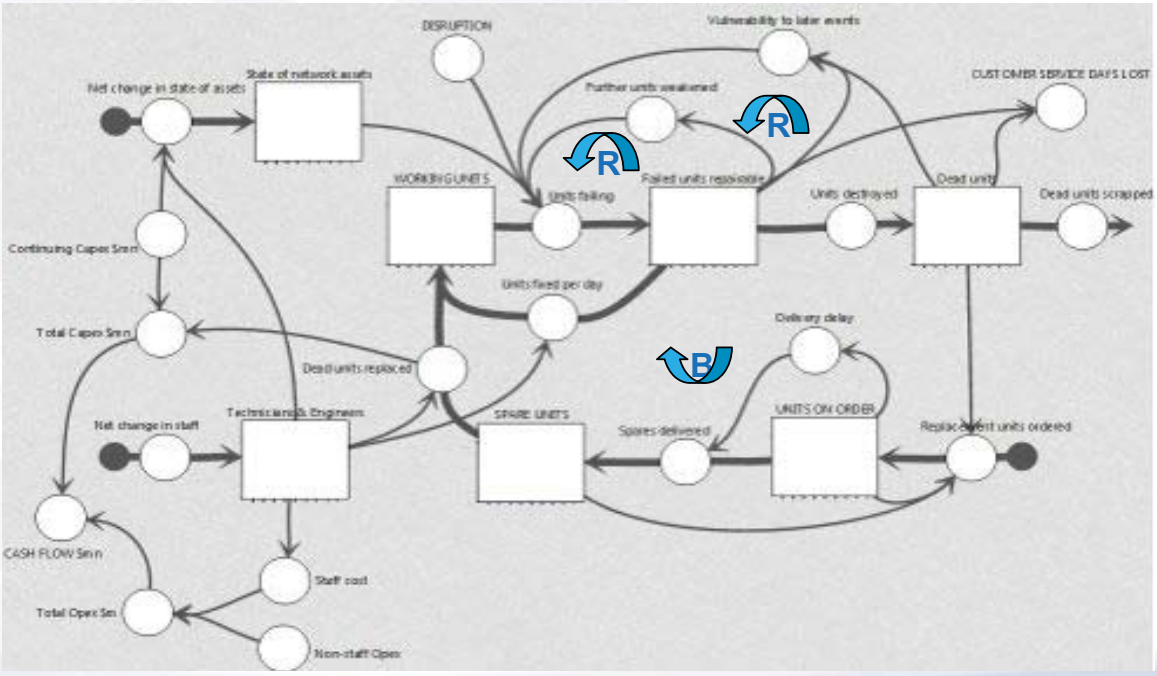
- The main weakness was a failure to explore in advance different risk scenarios, establish the probability of such scenarios occurring and put in place, also in advance, strategies that would mitigate the consequences and facilitate recovery.
- The challenge is that, since the source of threats is increasingly diverse, it is no longer sufficient to focus on making specific parts of the system resilient that are known to be at risk.
- Rather, strategy needs to raise the resilience of the whole network to whatever events might occur.
- The requirement to understand how a current situation has come about, the direction in which it might develop in future, and how to change that future for the better is not unique to risk and resilience, but is fundamental to all policy and strategy situations.

Resilience as a strategy/policy issue

- "Any improved approach to risk and resilience must be systemic in nature" (Pitt Review, HM Government, UK, 2007).
- The Pitt Review defined this requirement by several criteria:
  - It should consider the system as a whole, not just individual components or subsets in isolation.
  - The forces that cause the disruptive events and the events should themselves be part of the system.
  - It must capture the feedback between parts of the system (i.e. the effects caused by actions on the system can themselves be the cause of further effects).
  - It should recognise that actions can both improve the situation and make it worse (i.e. the feedback can be positive and negative).
  - Actions taken in advance to create or eliminate an effect may have delays in achieving this.
  - The effect of an action can change over time as the system changes.
  - The process of development and adaption of the system is continuous.

Risk & Recovery Assessment and Policy Modelling (systemic approach)

Risk / Resilience Model (main Feedback loop)



PROJECT STATUS

Two main Catastrophic Events have been chosen to be the object of the study:

- A terroristic attack to a transportation system
- An adverse weather-caused flood.

The first part of the analysis is now focusing on terroristic attacks: for these events, historical data has been collected, concerning in particular the 2004 Madrid and 2005 London bombings.

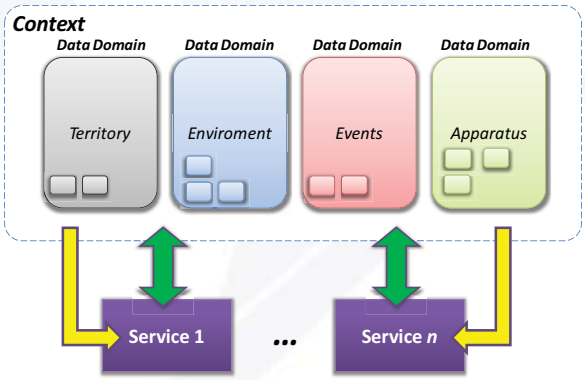
ONGOING ACTIVITIES

Attention is being focused now at the identification of an effective model to represent the Complex System of a large city, for the purposes of the project.

The current goals are:

- to Define a set of Data Domains that correctly represent the system (i.e. Territory, social environment, and so on);
- to Identify the key parameters of each Domain;
- to Define the relations between each Domain and the main Critical Infrastructures.

DATA DOMAINS



Describing a system through Data Domains like those pictured, allows for a first classification of all the parameters that influence a complex system into what we called **THEORETICAL MODEL**, and guides the first definitions of causal relations between parameters.

RESEARCH CHALLENGES

- Identify the common grounds between the different catastrophic events
- Improve Cis' risk and resilience policy development capabilities (as the threat of disruption to the CIs has increased and will continue to increase as the intensity of existing threats becomes greater and the diversity of sources for those threats widens)
- Identify different Risk Classes and the interdependencies between them and the CIs resilience
- Create a model that can be applied to many different European cities

IDENTIFYING THE COMMON GROUNDS BETWEEN THE DIFFERENT CATASTROPHIC EVENTS

Once the consequences of a specific catastrophic event have been identified, it will be necessary to determine which other catastrophic events will cause similar consequences on the CI system, and to what extent.

This will allow the creation of a series of best practices, that will guarantee mitigating effects in a wider range of critical events.

CREATE A MODEL THAT CAN BE APPLIED TO MANY DIFFERENT EUROPEAN CITIES

The consequences and behavior of catastrophic events in a given city are a direct consequence of a large number of variables representative of the city.

It will be necessary to create a model that will be both:

- detailed enough to take into consideration all the parameters that typify a city;
- simple enough to allow for an easy customization of such parameters.

PROJECT CONTACTS

Riccardo Onori – CRISADMIN Project Manager
onori@cattid.uniroma1.it

Stefano Armenia – CRISADMIN Technical Head
armenia@cattid.uniroma1.it

Proceedings of the CIPS II Workshop

Business Continuity Planning for Critical Infrastructures

Daniel Mosquera

ISDEFE

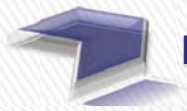
email: dmosquera@isdefe.es

Introduction to the CIPS-funded project, BUCOPCI

Contents of the presentation

- **BUCOPCI** – *What is it about?* – *[5 min]*
- **Project Structure** – *How are we managing the project?* – *[10 min]*
- **Project Status** – *Where are we and where are we going to?* – *[10 min]*
- **Stakeholder Group** – *Why having one?* – *[5 min]*
- **Conclusions** – *[5 min]*
- **Questions & Answers** – *[10 min]*

Bucopci



BUCOPCI

- **Definition and Objectives,**
- **BUCOPCI as part of the CIPS programme**
- **Consortium details**

BUCOPCI

BUCOPCI stands for:

Business Continuity Planning for Critical Infrastructures, but…

What is it about?

BUCOPCI

BUCOPCI

Objectives

*Identify best practices on **Business Continuity** and*

Security Planning.

BUCOPCI

Objectives

*Develop a **set of guidelines** on Business Continuity and*

*Security Planning **for Critical Infrastructure Operators.***

BUCOPCI

Objectives

***Increase awareness on Security and Business Continuity Planning** among Critical Infrastructure Operators from the transport sector.*

BUCOPCI

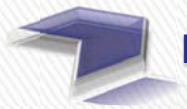
BUCOPCI as part of the CIPS programme

Objective 1 - Prevention and preparedness of risks.

- Stimulating, promoting and supporting the **development of methodologies** for the protection of Critical Infrastructures (CI), in particular risk assessment methodologies.

Objective 2 – Consequence management:

- Stimulating, promoting and supporting **exchange of knowledge** and experience, in order to establish best practices.



Project Structure

- Work Breakdown Structure
- Approach and Schedule
- Deliverables

Project Structure

Work Breakdown Structure

8 Work Packages

4 Technical-content

- ***WP1*** *– State-of-the-art Analysis*
- ***WP2*** *– Scenarios Definition*
- ***WP4*** *– Guidelines for Business Continuity Planning*
- ***WP5*** *– Guidelines for setting-up CIO Security Plans*

24 months project

Started on July 2011

End by July 2013

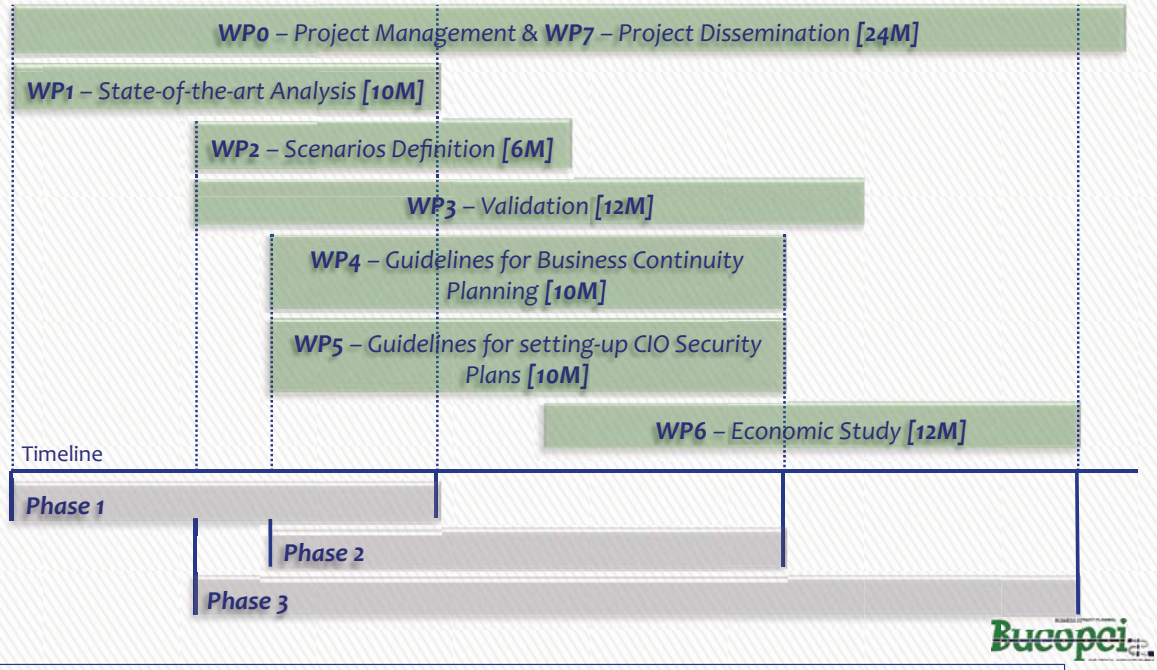
Executed in 3 phases

4 Transversal-activities.

- ***WP0*** *– Project Management*
- ***WP3*** *– Validation*
- ***WP6*** *– Economic Study*
- ***WP7*** *– Project Dissemination*

Project Structure

Approach & Schedule



Project Structure

Approach & Schedule

Phase 1

- Which are the accepted standards?
- What are the practices in BCP and OPS followed by Critical Infrastructures Operators?
- Is there a need for developing Guidelines for BCP and OSP?

Phase 2

- What are the end-users expectations?
- What are the "minimum contents" the Guidelines should have?

Phase 3

- Can we go beyond "theory"?
- Are Guidelines covering end-user expectations? Are they "fit-for-purpose"?
- Are Guidelines "cost-effective"?

Project Structure

Work Breakdown Structure

***WP1** – State-of-the-art Analysis*

- Review of **international standards** in **Business Continuity Plan** (e.g. BS-25999-1, BS-25999-2), **Contingency Planning-IT** (e.g. ISO-24762, SS-507, ITIL, ISO-20000), **Disaster Recovery Plan-IT** (e.g. ISO-27002, NIST 800-34, ISO 24031, ISO-27001)
- Assessment of **current implementation of BC and OSP** to Critical Operators in Transport Sector (via CNPIC)
- Identification of **Common Continuity Practices** in Critical Operators.

Deliverables

- d1.1 – Standards Analysis Report (Public domain)
- d1.2 – Business Continuity Best Practices Report (Public domain)
- d1.3 – Security Plan Best Practices Public (Public domain)

Project Structure

Work Breakdown Structure

***WP2** – Scenarios Definition*

- Describes **disruptive chain of events**, Triggered through malware; Potentially **initiated as an act of cyber terrorism**.
- **Focused on IT infrastructure** of transport sector.
- Developed to **validate the guidelines**.
- Built from the **stakeholder requirements/expectations**.

Deliverables

- d2.1 – Report On Scenarios Definition (Public Domain)

Project Structure

Work Breakdown Structure

***WP3** – Validation*

- Aimed at demonstrating that guidelines as developed in WP4 and WP5 are **fit for purpose**
- Limited to validate the benefits that **using the guidelines** could bring and not the benefits **that applying a BCP and OSP** as developed with such guidelines could bring
- Defines validation objectives **from stakeholders expectations**
- Follows the **European Operational Concept Validation Methodology (E-OCVM)**

Deliverables

- d3.1 – Validation Strategy (Project-restricted)
- d3.2 – Validation Report (Public Domain)

Project Structure

Work Breakdown Structure

***WP4** – Guidelines for Business Continuity Planning*

- Built following the **Business Continuity Management Cycle** and presented in 4 chapters:
  - Understanding the organization, Determining Continuity Strategy, Development and implementation of BCM, Practices, Maintenance and Review.
- **Theoretical and Practical Sections**. Step-by-step guide explaining the methodology implementation
- **Extended information** with specific information on implementation.

Deliverables

- d4.1 – Business Continuity Planning Guidelines (Public Domain)

Project Structure

Work Breakdown Structure

***WP5** – Guidelines for setting-up CIO Security Plans*

- Starts from an **analysis of European and National regulations** linked to CI Operators Security Plans.
- Includes: Security governance framework, Essential services identification and Risk analysis methodologies
- Aimed to **facilitate the identification and protection** of critical components within Critical Infrastructures.

Deliverables

- d5.1 – Operator Security Plans Guidelines (Public Domain)

Project Structure

Work Breakdown Structure

***WP6** – Economic Study*

- Aimed at **demonstrating the cost-efficiency** of Guidelines implementation.
- Will **compare** the costs (**qualitative**) of developing BCP and OSP with and without using the guidelines.
- Built on the assumption that plans developed with or without guidelines are equally correct and their implementation yields to the **same recovery times**.
- Built from, at least, one of the **scenarios defined in WP2**.

Deliverables

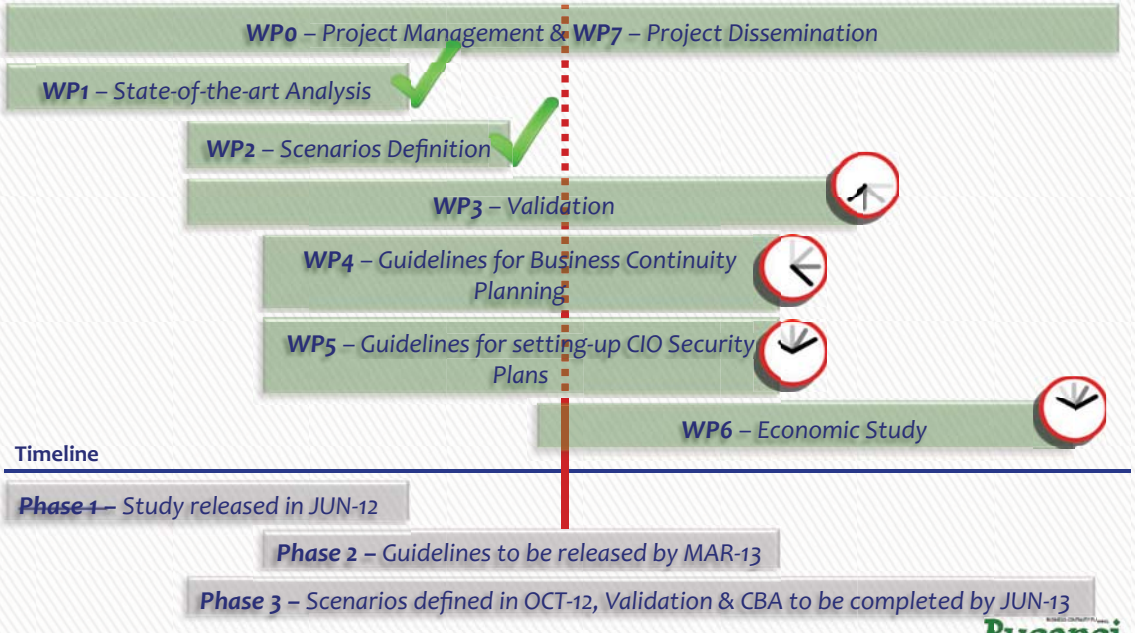
- d6.1 – Business Impact Analysis

Project Status

- **Where are we and where are we going to?**
  - **Phase 1 - Results obtained.**
  - **Phase 2 & 3 - Results obtained so far.**

Project Status

Where are we and where are we going to?



Project Status

Phase 1 - Results obtained.

Phase 1 *– Study released in JUN-12*

WP1 *– State-of-the-art Analysis*

Together, BCM and OSM standards, allow a Global Risk Management by:

- An **establishment of policy** and objectives to manage risks.
- A **better understanding and prioritisation** of important activities and organization's risk, security, preparedness, response, continuity and recovery requirements.
- A **broader view of risk** and more pragmatic risk treatment. A better view of evolving threats and risks.
- Better **Access to Executive Boards** to improve investments in security and business continuity

Release of: d1.1 – Standards Analysis Report (Public domain)

Project Status

Phase 1 - Results obtained.

Phase 1 *– Study released in JUN-12*

WP1 *– State-of-the-art Analysis*

The **compliance of BCM is not appropriate.** There are methodological aspects that have not been covered in the current cycle of Operator BCM Cycle.

- There are some aspects concerning *Understanding the Organization, Determining Business Continuity Strategy and Developing and implementing BCM Response,* **where the effort should be concentrated**.
- There are some others, such as *Exercising, maintaining and reviewing BCM arrangements, Embedding BCM in the Organization Culture and BCM Policy and Programme Management,* **where could be improved.**
- **Business Continuity Management has not been recognized as strategically important.**

Release of: d1.2 – Business Continuity Best Practices Report (Public domain)

Project Status

Phase 1 - Results obtained.

***Phase 1** – Study released in JUN-12*

***WP1** – State-of-the-art Analysis*

The **compliance level of OSM is high** and therefore there is a good level of maturity.

- A **governance structure is defined** to organizing information security within and across the organization.
- **Procedures are communicated to individuals** who are required to follow them.
- IT security **procedures and controls are implemented** in a consistent manner everywhere that the procedure applies.
- Physical and Environmental Security practices, technologies and services are implemented to **protect information assets and the premises in which they reside**

Release of: d1.3 – Security Plan Best Practices Public (Public domain)

Project Status

Phase 2 - Results obtained so far.

***Phase 2** – Guidelines to be released by MAR-13*

***WP4** – Guidelines for Business Continuity Planning*

***WP5** – Guidelines for setting-up CIO Security Plans*

Stakeholders requirements have been captured, prioritized and implemented:

- Guidelines should **be flexible enough to be adapted to any transport sub-sector** instead of being sector oriented,
- Guidelines should **be aligned with international standards** and more over with **international regulations**
- Guidelines should **be focused on resilience**
- Guidelines should **be cost-efficient**, i.e. be effective and save time and money when using them

Project Status

Phase 2 - Results obtained so far.

***Phase 2** – Guidelines to be released by MAR-13*

***WP4** – Guidelines for Business Continuity Planning*

Guidelines for Business Impact Analysis about to be released.

***WP5** – Guidelines for setting-up CIO Security Plans*

Study of European and National regulations linked to CI Operators Security Plans already done.

Guidelines will be released during the second half of the project

Project Status

Phase 3 - Results obtained so far.

***Phase 3** – Scenarios defined in OCT-12, Validation & CBA to be completed by JUN-13*

***WP2** – Scenarios Definition*

- **Scenario 1:** Cyber terrorism attach on the Air Traffic Control System.
- **Scenario 2:** Disruption of international courier supply chain through failure of the control system for runway lighting.

***WP3** – Validation*

- **V01:** Guidelines should be flexible enough to adapt their output to any specific critical transport sector.
- **VO2:** Guidelines should be cost-efficient so they can save time and money when using them.

***WP6** – Economic Study*

Results on WP6 are expected for the second half of the project.

Release of: d2.1 – Scenarios Definition Report (Public domain)
Release of: d3.1 – Validation Strategy (project-restricted)

Stakeholder Group

- **Why having one?**
  - **Members**
  - **Meetings**

Stakeholder Group

Why having one?

- **Expertise** in BCP/OSP is critical
- **Best practices** should be identified
- **Expectations** from guidelines should be covered
- **Realistic** scenarios must be defined
- Validation should be **done by experts**
- Guidelines should go **beyond theory**

Stakeholder Group

Members

Transport sub-sector	Organization
Air Transport	Cork Airport / Dublin Airport Authority (Ireland)
	AENA – Spanish Airports and Air Navigation (Spain)
	EUROCONTROL HQ (Brussels)
	CASSIDIAN (France)
Rail Transport	RENFE (Spain)
Sea Transport	Puertos del Estado (Spain)
Intermodal Transport	DHL Supply Chain (Spain)
CI Authority	CNPIC (Spain)

Introduction to the CIPS-funded project BUCOPCI.

Stakeholder Group Meetings

WP0** – Project Management & **WP7** – Project Dissemination **[24M]

***1st SGM** – APR13*
- Second Guidelines validation session

***2nd SGM** – NOV/DEC12*
- First Guidelines validation session

Timeline

***1st SGM** – JUL12*
- *Capture the stakeholder's expectations*
- *Identify best practices in BCM & CI OSP*

***1st SGM** – JUL13*
- Final workshop (Madrid)

Introduction to the CIPS-funded project BUCOPCI.

Conclusions

Things you have to keep in mind.

- Guidelines developed in BUCOPCI will be **of public domain**.
- **Critical Infrastructures Operators** in the transport sector in Spain, have contributed to the common practices identification.
- Guidelines should be **flexible enough to** adapt their input to any transport sector.
- Guidelines have been **built from the stakeholders expectations**, and will be **validated by the stakeholders** at the end of the project.
- Final **workshop will be held at Madrid** by July 2013, if you want to attend please contact us.
- **BUCOPCI is no yet finished**, in the following 5 months most of the expected results should be released.
- The **Stakeholder Group is "dynamic"**, if you want to join, please let us know.

BUCOPCI

Consortium details

- **Isdefe**. Ingeniería de Sistemas para la Defensa de España – Spain.
- **SIA**. Sistemas Informáticos Abiertos – Spain.
- **Vicomtech**. Fundación Centro de Tecnologías de Interacción Visual y Comunicaciones – Spain.
- **WIT**. Waterford Institute of Technology – Ireland
- **CNPIC**. Centro Nacional para la Protección de las Infraestructuras Críticas – Spain.

Introduction to the CIPS-funded project BUCOPCI.

Contact Details

Contact,	For,	At,
Daniel Mosquera **Isdefe**	Project queries on: 1) Validation, Dissemination, Management, Stakeholder Group, etc.	coordinator@bucopci.eu dmosquera@isdefe.es
Daniel Blanco **SIA**	Technical queries on: 1) State-of-the-art Study 2) Guidelines for Business Continuity Planning	dblanco@sia.es
Diego Fernández **Isdefe**	Technical queries on: 1) Guidelines for CI Operator Security Plans	dfernandez@isdefe.es

Visit us at: **www.bucopci.eu**

Follow us at: **http://www.linkedin.com/groups?about=&gid=4341688**

Partners

Project Coordinator

Isdefe (www.isdefe.es)
Daniel Mosquera-Benitez
dmosquera@isdefe.es

Associate Member

Associate Member:
CNPIC (www.cnpic-es.es)

Co-beneficiaries

Vicomtech (www.vicomtech.es)
Seán Gaines
sgaines@vicomtech.org

SIA (www.sia.es)
Daniel Blanco
dblanco@sia.es

WIT (www.wit.ie)
Robert Mullins
rmullins@tssg.org

Proceedings of the CIPS II Workshop

Security Risk Management Processes for Road Infrastructures

Harald Kammerer

ILF Consulting

email: Harald.Kammerer@ilf.com

Security Risk Management Processes for Road Infrastructures

Harald Kammerer, MSc
ILF Consulting Engineers, Austria

Outline

SECMAN
Security Risk Management Processes for Road Infrastructures

- Introduction
- Methodology
- Output till now
- Future tasks
- Questions and Answers

Introduction

- Recent Incidents


TOPNEWS.DE

Jenaer Autobahntunnel nach Bombendrohung gesperrt

Verdächtiger Gegenstand erwies sich als Attrappe

Jena (ddp-th). Nach einer Bombendrohung ist der Jenaer Lobdeburgtunnel auf der Autobahn 4 am Samstag für vier Stunden gesperrt worden. Nach Angaben der Polizei hatte ein unbekannter Anrufer am Morgen mit der Zündung eines

POLIZEI

A4, Germany – September 2009

A57, Germany – Februar 2012

Introduction

- Recent Incidents

Wiehltal bridge, Germany – Aug. 2004

Viamala tunnel, Switzerland – Sept. 2006

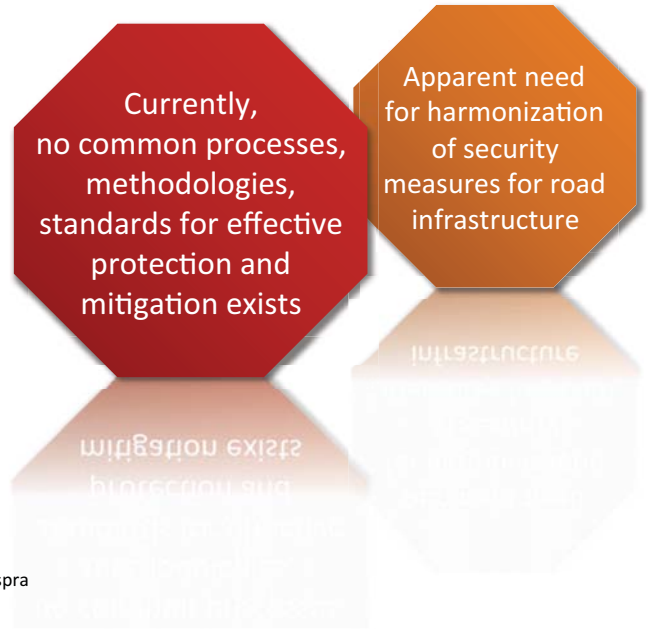
Introduction

- Motivation for the project

1. The importance of the European transport network for our economy and society.
2. Possible risk for disturbance of the critical road infrastructure like bridges, tunnels, … and potential disconnection of the European transport routes.
3. Consecutive negative consequences for the population and the economy.

Introduction

- Current situation



Introduction

- Objectives

1. To develop a practical process for the identification of critical infrastructures in Europe
2. To assess these infrastructures in a structured and comparable way
3. To determine the effective protection and mitigation measures
4. To summarize all ascertainments in a comprehensive best-practice manual for owners and operators of road infrastructures in Europe

Introduction

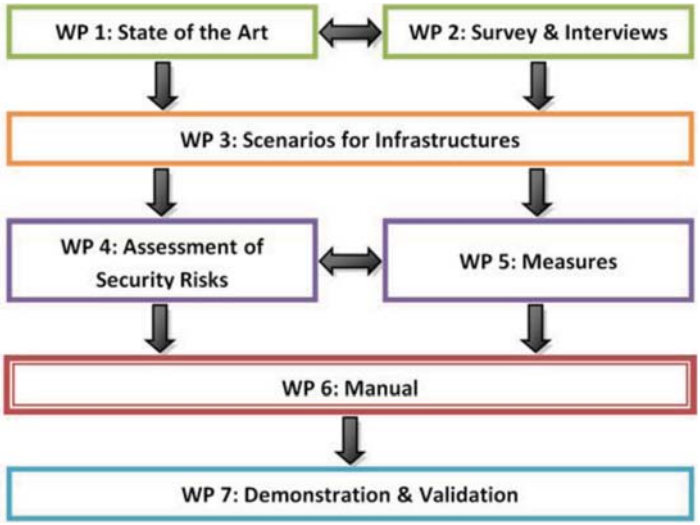
- Benefits

The manual gives the possibility to…

1. …define priorities with respect to critical infra-structures by the elaboration of a ranking system
2. …increase the awareness of weak points of specific infrastructure in relationship to existing threats
3. …propose a set of possible measures for a specific object (type) with respect to existing threats

Introduction

- Project structure



Introduction

- Project structure (cont.)

WP 1

State of the Art:

Analysis of the state of the art regarding current and completed research projects as well as relevant literature

WP 2

Survey & Interviews:

Survey and interviews with owners and operators of road infrastructures regarding security risk management for bridges and tunnels

WP 3

Scenarios for Infrastructures:

Identification of relevant infrastructure specific scenarios based on existing threat analyses

Introduction

- Project structure (cont.)

WP 4	WP 5	WP 6
Assessment of Security Risks: Methodology for the - identification, - quantification, - analysis and - assessment of security risks	Measures: Recommendations for structural, operational and organizational prevention/ mitigation measures with estimation of their effectiveness	Manual: Preparation and elaboration of a substantial security risk manual for road infrastructures

Introduction

- SecMan consortium

bast	iLF	DARS	Elea iC
Federal Highway Research Institute (Germany)	Consulting Engineers (Austria)	Motorway Company in the Republic of Slovenia (Slovenia)	Consulting Engineers (Slovenia)

www.secman-project.eu

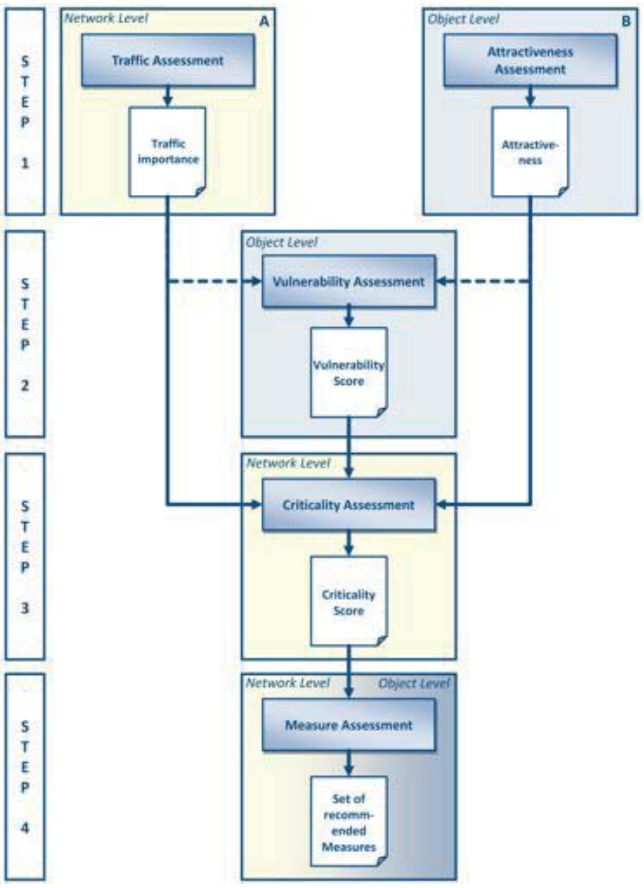
Methodology

- 3 main problems for a methodical approach…

Problem 1	Large number of objects in a road network	**Preselection Method**
Problem 2	High complexity due to a great amount of different threats and objects	**2-Level approach**
Problem 3	General applicability of default values for a simplified approach	**allow user modifications**

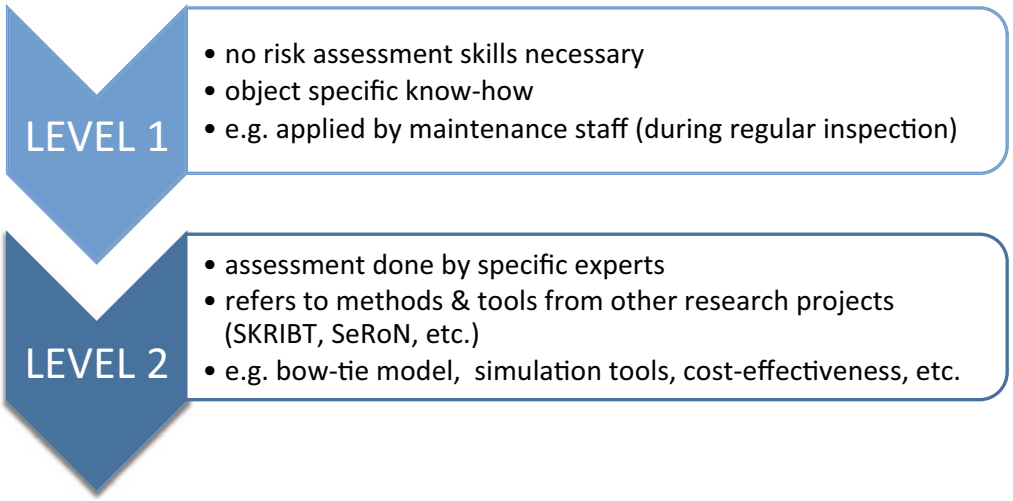
Methodology

- 4-step procedure
- Object / Network Level
- 2 Level approach in terms of complexity
- Specific data necessary
  - General traffic data
  - Infrastructure data



Methodology

- 2 Level approach



Output till now

WP 1	State of the Art	**Finished**
WP 2	Survey and Interviews	**Finished**
WP 3	Scenarios for Infrastructures	**Finished**
WP 4	Assessment of Security Risks	**Partly Finished**
WP 5	Measures	**In Progress**

Output till now

SECMAN
Security Risk Management Processes for Road Infrastructures

WP 1

1 **SKRIBT:**
Protection of Critical Bridges and Tunnels on Roads

2 **SeRoN:**
Security of Road Transport Networks

SECMAN
Security Risk Management Processes for Road Infrastructures

Output till now

WP 2

- **Survey**
  - Owners and Operators of road Infrastructures in Europe
  - Feedback not quantifiable, **BUT:** some general conclusions
- **Interviews**
  - Follow-up on interesting responses from the survey
  - More in-depth

Output till now

SECMAN
Security Risk Management Processes for Road Infrastructures

WP 3

- Elaboration of relevant THREATS for tunnels and bridges

Threats – Tunnels				
Explosion	**Fire**	**Mech. impact**	**Sabotage**	**Cyber**
Small Explosion (20 kg TNT)	Arson	Projectiles		
Medium Explosion (100 kg TNT)	Major Fire (150-200 MW)			
Major Explosion (2 t TNT)				
BLEVE (18 t Propane)				

Threats - Bridges			
Explosion	**Fire**	**Mech. impact**	**Sabotage**
Small Explosion (20 kg TNT)		Ramming	
Medium Explosion (100 kg TNT)			
Major Explosion (2 t TNT)			

SECMAN
Security Risk Management Processes for Road Infrastructures

Output till now

WP 3

- Definition of initial threat scenarios
- Categorization of infrastructures

Tunnels	Bridges
Predominant geotechnical conditions	Static system
Construction method	Span / height
Hydrological conditions	Construction material
Single shell vs. Dual shell	Superstructure section
Single cell vs. Multiple cells	

18 tunnel types
19 bridge types

Output till now

SECMAN
Security Risk Management Processes for Road Infrastructures

WP 4

- *Finished*: **Vulnerability Assessment**

BRIDGE - Type No. B01										
			Feasibility of Attack							
		Damage Potential	object specific knowledge	technical knowledge	acquisition of material	access & transport	trigger event	TOTAL	VULNERABILITY	Additional comments
Explosion	Small	2	1	1	1	0	1	4	8	Access to bearings at small bridges more difficult due to narrow space at access points
	Medium	6	0	0	1	0	1	2	12	
	Major	12	1	0	0	1	1	3	36	
Fire		12	1	1	1	1	1	5	60	-
Mech. Impact	Ramming	0	1	0	0	0	0	1	0	-
Sabotage		0	0	0	0	0	0	0	0	-
									116	

- *Pending*: **Criticality Assessment**

SECMAN
Security Risk Management Processes for Road Infrastructures

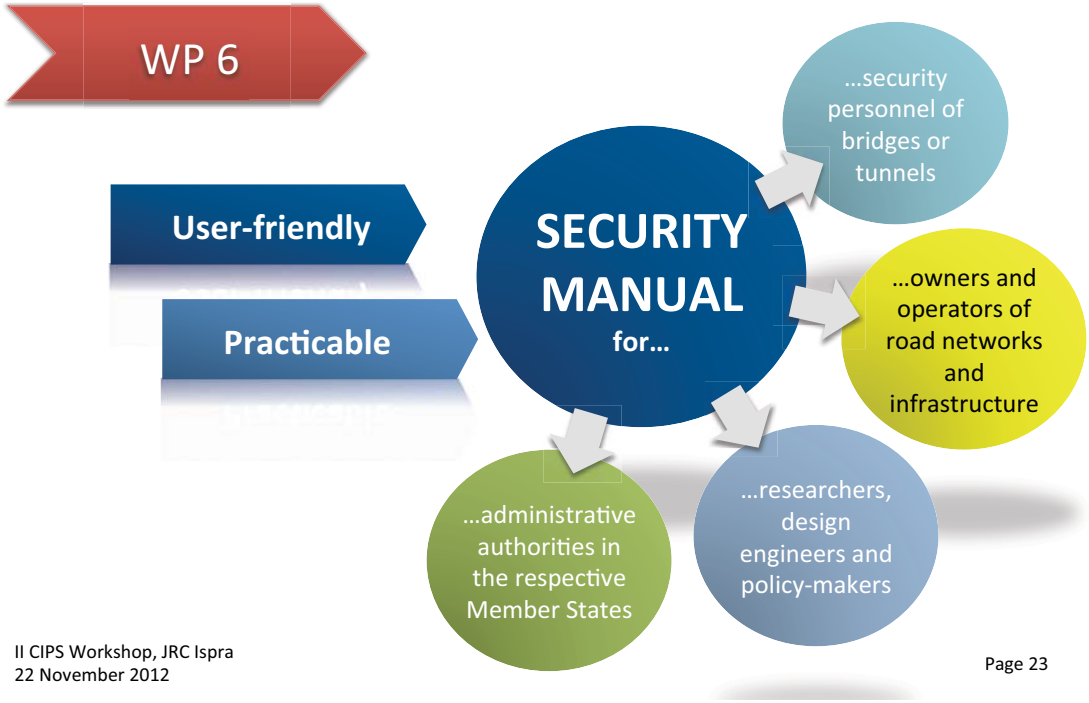
Future tasks

WP 5

- Representation of Measure(s) for
  - a specific **object**,
  - addressing individual **threats**
  - to reduce either the **damage potential** or **feasibility of attack** and
  - to protect **humans** and **structure**
  - and ensure **traffic flow**

- NO detailed evaluation of measure effectiveness in relationship to vulnerability, criticality or costs!

Future tasks



Future tasks

WP 7

- Validation & Demonstration of the SecMan user manual
  - Bridge over river Inn (GER/AUT)
  - Karawanken tunnel (AUT/SLO)

SECMAN
Security Risk Management Processes
for Road Infrastructures

Questions and Answers

SECMAN
Security Risk Management Processes
for Road Infrastructures

II CIPS Workshop
JRC Ispra – 22-23 November 2012

Security Risk Management Processes for Road Infrastructures

Harald Kammerer, MSc
ILF Consulting Engineers, Austria

Development Of a Risk Assessment methodology to Enhance security Awareness in ATM

Palma Altieri

SESM

email: paltieri@sesm.it

With the financial support of the CIPS Programme
EC – DG Home Affairs

Development Of a Risk Assessment meTHodology to Enhance security Awareness in ATM.

SESM
A Finmeccanica Company

DORATHEA

gmv
INNOVATING SOLUTIONS

Outline

- **Partnership**
- **DORATHEA Project**
- **A new methodology**

SESM
A Finmeccanica Company

- Founded in 1990, SESM is a private research centre owned by
  - **SELEX Sistemi Integrati** (world leader in the design and development of innovative solutions to ensure efficiency and safety in Air, Airport and Coastal Traffic Management) and
  - **SELEX Galileo** (world leader in defence electronics markets, with a distinctive strength in airborne mission critical systems and homeland security applications).
- SESM is part of Finmeccanica Group, based in Naples (HQ) and Rome.
- SESM's research activities focus on the development of information solutions by adopting state-of-art information and communication technologies.



SESM
A Finmeccanica Company

- **Mission**
- SESM operates in the design and development of Decision Support and Knowledge Based Systems.
- SESM has 120 employees, most of them research engineers.
- SESM main domain of activities are:
  - Middleware and Open-Source for mission-critical systems
  - Interoperability for Air Traffic Management and Crisis Management
  - Security and Dependability for Embedded Systems certification and Critical Infrastructure protection
  - Radar Tracking and Data Fusion for surveillance systems
  - Integrated logistic support for complex systems maintenance



- Multinational conglomerate founded in 1984
- Offices in Spain, Portugal, Poland, USA, Germany, Romania, Malaysia, and India
- Permanent staff in 10 countries

$140M (total revenue)

Over **1.000 employees** worldwide

CMMI Level 5

- GMV has deep knowledge in key technologies for Aeronautics:
  - CNS / ATM Technologies and Data Fusion
  - Airport Security Systems Integration
  - Flight Physics & Control Techniques implementation
  - GNSS/INS navigation systems development
  - Embedded Systems (SW/HW) & Integrated Modular Avionics, IMA
  - Safety Critical Software and Certification
  - Aircraft Simulation
- Combined with Defence technologies:
  - Communication systems
  - C4I and ISTAR systems
  - SIGINT
- Reference Clients include
  - AENA, Eurocontrol, Airbus Military, Embraer, Thales, EADS, …

Introduction to DORATHEA

- **Call for proposals:** CIPS 2010 – DG HOME
- **Registration number:** HOME/2010/CIPS/AG/030
- **Name of the Applicant organisation**: SESM Scarl (Italy)
- **Partners/co-beneficiaries**: GMV SKYSOFT, S.A. (Portugal)
- **Duration of the project**: 24 months
- **Total eligible costs (EUR)**: 572.028,92
- **Grant (EUR):** 400.134,22 (69,95%)

DORATHEA is related to the ATM CI Protection

Security in ATM

- ICAO's Security Manual for Safeguarding Civil Application
  - helps in identifying and prioritising threats according to time and budget constraints.
  - It is more related to the Airport Security Management and Airborne Security.
- New guidelines comes from SESAR (SWP 16.2)
  - The out-coming methodology is mostly based on the definition of security cases
  - It is limited to the operative context of SESAR.

A Common Methodology for the Security Risk Assessment of ATM-CI needs to be defined

DORATHEA's Objectives (1/2)

- The objective of DORATHEA is the development of a common methodology for carrying out risk, threat and vulnerability assessments for ATM Critical Infrastructures (ATM-CI) protection.

- Why is it important to develop a common methodology for the Security Risk Assessment of ATM-CI?
  - To have a coherent implementation of measures to protect European ATM critical infrastructure
  - To clearly define the respective responsibilities of all relevant stakeholders.

DORATHEA's Objectives (2/2)

The security risk assessment methodology developed in DORATHEA will:

- extend and be consistent with consolidate standards already in usage
- address either new ATM-CI system as well as legacy system and assess the risk deriving from their connection
- give effective guidance to identify protection measures.
- **be proposed as a common security baseline for all EU ATM systems**

WHY CIPS?

- The methodology will be developed and validated through interviews and workshops with key players.
- **SESM** and **GMV** will carry out the former activities, assisted by **Project Advisory Committee (PAC)**.
- The **Target Group (TG)** will be involved to achieve the **dissemination** objectives and to collect **feedbacks**.

ATM stakeholders

National Supervisory Authorities

Air Navigation Service Providers

Planned Workshops

- Jenuary 2013 in Bruxelles
  - **Vulnerabilities assessment**

- June 2013 in Rome
  - **Countermeasures identification**
- December 2013 in Lisbon
  - **Final public dissemination**

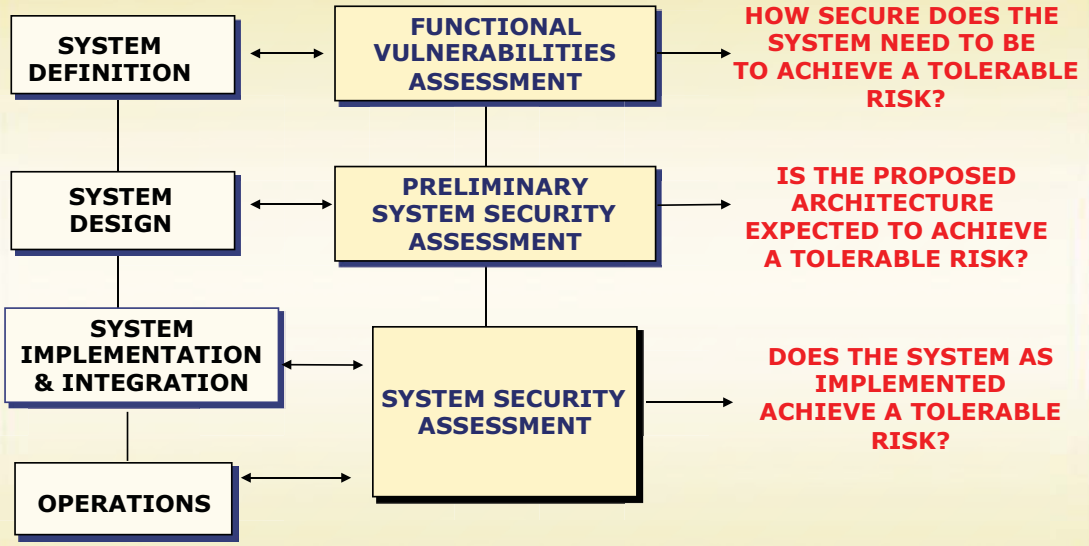
DORATHEA Methodology - Innovative aspects

- **Identification of vulnerabilities**
  - will take into account weak points that will arise from the integration of legacy ATM systems and new ATM system
- **Threats analysis**
  - will explore possible connection or threat propagation from other ATM subsystems
- **Risk assessment**
  - will produce a quantitative and qualitative measure of the risk
- **Identification of countermeasures**
  - will propose enhancements to the ATM security

DORATHEA Methodology - A SAM for Security

- Safety Assessment Methodology (SAM) is a guideline that became a standard de facto well before EC Regulations put into force ESARRs.
- It preserves the distinction of roles and responsibilities:
  - **ANSPs**, responsible for operations, have the first and the last word
  - **Stakeholders**, who have the knowledge of equipment, have to identify Safety Requirements.
- There is the need for a security methodology similar to SAM, in which to **ANSPs** is left the responsibility to identify **Security Objectives**, starting from the knowledge of operational environment.

Security Assessment Process



Security Assessment is the mean of providing assurance that a system is secure for operational use.

Functional Vulnerability Analysis (1/2)

- **ANSPs** have the responsibility of this phase.
- **For each identified vulnerability the *Security Objective* specifies the maximum tolerable likelihood of its occurrence, given its assessed severity.**

A definition of Security Risk is needed

- **Safety Risk** = $P_e * P_h * S_c$
- **Threat** is the Event that triggers the Vulnerability, which corresponds to a Hazard.
- **Vulnerability** corresponds to loss or corruption of functionalities, which occur when a Threat is in place.
- **Security Risk** = $L_t * L_v * S_c$

Functional Vulnerability Analysis (2/2)

- Through a functional analysis, ANSPs have to identify potential security incidents.
- Through the **security risk matrix**, Likelihood can be fixed, according to the known Severity.

		LIKELIHOOD OF OCCURRENCE				
		Extremely improbable	Extremely remote	Remote	Reasonably probable	Probable
SEVERITY CLASS	I Catastrophic					
	II Hazardous					
	III Major					
	IV Minor					
	V No Effect					

Acceptable | Tolerable | Unacceptable

Preliminary System Security Assessment

- **Stakeholders** have the responsibility of this phase.
- Through a **Threat Tree Analysis** (functional analysis) and a **Failure Mode and Effect Analysis** (physical analysis), elementary threats can be identified.
- For each relevant threat, one or more **security controls** have to be identified.
- These security controls can be traced to **System Requirements** to become **Security Requirements**.

System Security Assessment

- **Stakeholders** have to demonstrate the correct implementation of security controls.
- **Security metrics** are introduced:
  - SMART Specific, Measurable, Achievable, Repeatable, Time-dependent
  - Measurement enables improvement: Security metrics is to improve the maturity and effectiveness of the overall security program, while demonstrating cost-effectiveness.
- **Verification of Security Requirements**.

Development strategy

- Evaluate the state of the art of the risk assessment methodology for ATM-Ground and Air-Ground systems by the study of literature, standards and rules
- Create functional models of the systems used in the ATM by interviews with stakeholder
- Develop the methodology on the basis of the results of previous activities
- Identify and classify security vulnerabilities by the application of the methodology and the results of workshop and interviews
- Identify and classify security threats by the application of the methodology and the defined models
- Identify security countermeasures by the application of the methodology and results of workshop and interviews
- Validate the methodology and refine/improve it by interviews with regulators

Scenario of validation

- **Airport air-side**
- Selection of phases of gate-to-gate cycle:
  - Approaching
  - Landing
  - Routing on the ground
  - Parking
  - Push-back
  - Routing toward runways
  - Holding before entering runways
  - Take-off
- The above phases involve the use of data-link, communication, A-SMGCS systems, etc..
- Main actors involved are: ATC, Pilots and Airlines, Airport Authorities.
- Security Risks are "relevant", many systems involved.

What after DORATHEA?

- SESM and GMV will extensively apply the methodology to EU and national projects, thereby the methodology will be consolidated.
- After the end of the project the vulnerabilities and threats identified for the different ATM systems will be stored in a database that represents a "knowledge base".
- The knowledge base will collect valuable information to:
  - open new research activities
  - evaluate the evolution of security awareness
  - improve countermeasures.
- SESM and GMV will push the methodology to make it a standard at EU level.

Contact details

SESM Scarl
Via Circumvallazione Esterna – Loc. Pontericcio
80014 Giugliano in Campania (NA) Italy

Palma Altieri
paltieri@sesm.it
phone +39.081.8180395

Proceedings of the CIPS II Workshop

Critical ICT Infrastructures Simulation of Interdependency Model II

Julio Vivero Millor

GMV

email: jvivero@gmv.com

2nd CIPS WORKSHOP

CISIM

CODE: GMV-CISIM-PRE-2ndCIPSWorkshop
DATE: 22/11/2012
VERSION: 1
JRC – ISPRA (ITALY)

Secure e-Solutions®
GMV SOLUCIONES GLOBALES INTERNET S.A.U.

UNCLASSIFIED

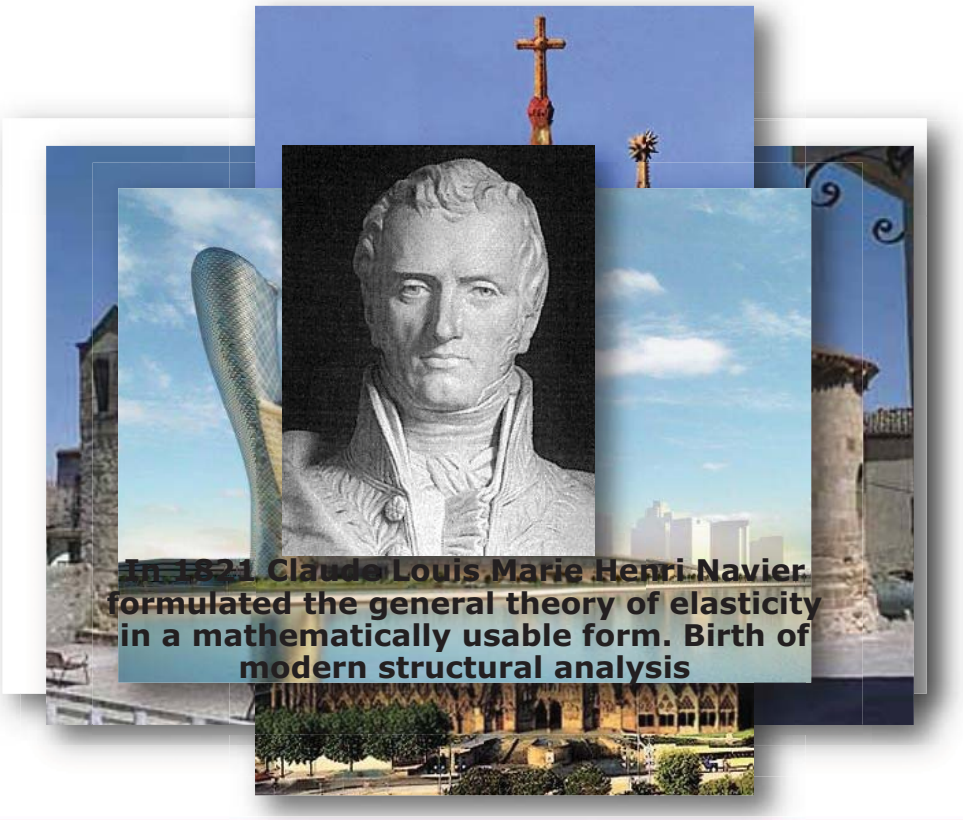
gmv INNOVATING SOLUTIONS

2nd CIPS WORKSHOP

CISIM:

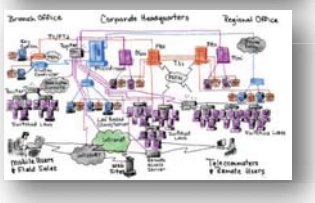
Critical ICT Infrastructures Simulation of Interdependency Model

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme"
European Commission - Directorate-General Home Affairs



PROBLEM DESCRIPTION

- Our reliance on ICT infrastructure grows.
- Complexity increases
- Threats rise:
  - Hacktivism
  - Cyberwarfare
  - …



PROBLEM DESCRIPTION

- and yet:

There is no mathematical model for calculating the dependability of an ICT infrastructure.

INDEX

CISIM – 2nd CIPS WORKSHOP

CONSORTIUM

UNCLASSIFIED INFORMATION

INNOVATING SOLUTIONS

CONSORTIUM

5

BACKGROUND

UNCLASSIFIED INFORMATION

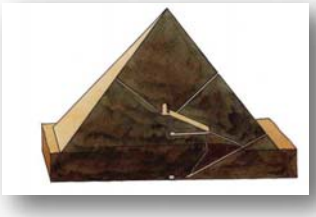
BACKGROUND

- RAMS:
  - **R**eliability
  - **A**vailability
  - **M**aintainability
  - **S**afety
- At design phase
- Why?:
  - Expensive missions
  - Unfeasibility of repairing broken components
  - Limitations of size and weight

BACKGROUND - II

- In ICT:
  - Redundancy, replication, backup and other contingency measures are significantly easier and cheaper to apply…

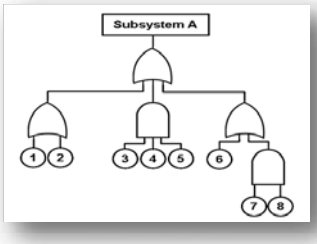
    THE PYRAMIDS APPROACH



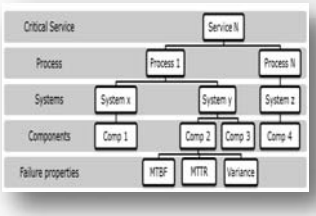
- With the rise of complexity and dependability on ICT the "Pyramids Approach" is:
  - Increasingly expensive
  - Too uncertain

BACKGROUND - RAMS

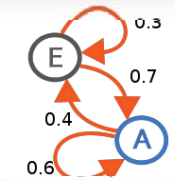
- Combination of:
  - Analysis of system failures and impacts to obtain:
    - MTTR
    - MTBF



  - Infrastructure modeling:
    - Effects of failures on the service provided by the infrastructure.



  - Calculation:
    - Markov Chains: Limit in infrastructure complexity
    - Simulations: Limit in processing time



BACKGROUND - CRICTISIM

CRICTISIM

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme" European Commission - Directorate-General Home Affairs

- RAMS applied to ICT
- Forecasting of ICT infrastructure dependability.
- At design and operational phase:
  - Sensitivity analysis
- Failure events:

Hardware	Software	Location damage
Human dependability	Network	Cyberthreats

BACKGROUND – CRICTISIM RESULTS

CRICTISIM

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme" European Commission - Directorate-General Home Affairs

- Results:
  - MIMICS (Modeling Infrastructure Method for ICT Critical Systems)
  - Forecast of ICT resilience
  - Identification of resilience bottlenecks
  - Investment optimization

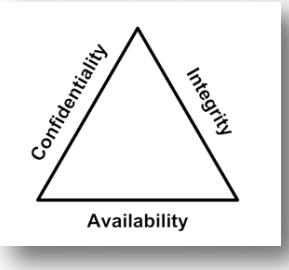
CISIM GOALS

UNCLASSIFIED INFORMATION

INNOVATING SOLUTIONS

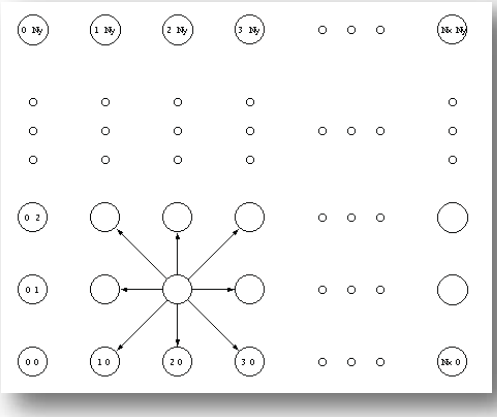
CISIM GOALS

- Forecasting of big infrastructures:
  - New mathematical models
  - Fast simulation techniques
- Infrastructures inter-dependability
  - External services dependencies
  - Domino effect
  - Large inter-dependencies simulations
- Feasibility study to forecast:
  - Confidentiality
  - Integrity



BIG INFRASTRUCTURES

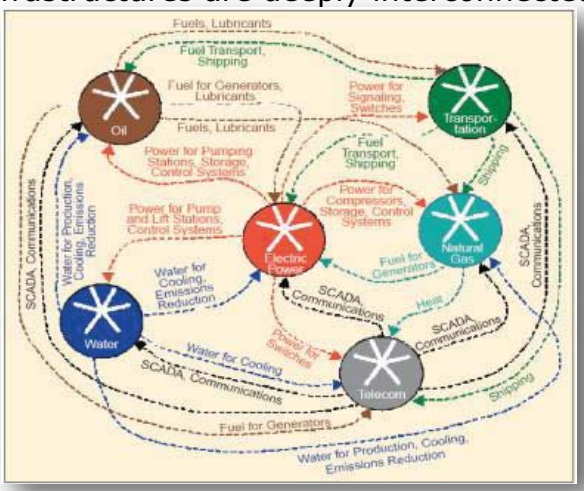
- Forecasting of big infrastructures:
  - Big and complex infrastructures is where forecasting is more valuable
  - Interconnected infrastructures form a complex eco-system



Requires innovative fast simulation and markov chain techniques.

INTER-DEPENDABILITY

- Infrastructures inter-dependability:
  - Modeling not only internal failure events but also external ones
  - Critical infrastructures are deeply interconnected.



Source paper: "System-of-systems" approach for interdependent critical infrastructures" - Irene Eusgeld, Cen Nan, Sven Dietz -ETH Zurich

FEASIBILITY STUDY

- Feasibility study for Confidentiality and Integrity forecasting:
  - Important properties in Critical Infrastructures
  - Lack of Confidentiality or Integrity can result in lack of availability

CISIM – 2nd CIPS WORKSHOP

APPROACH

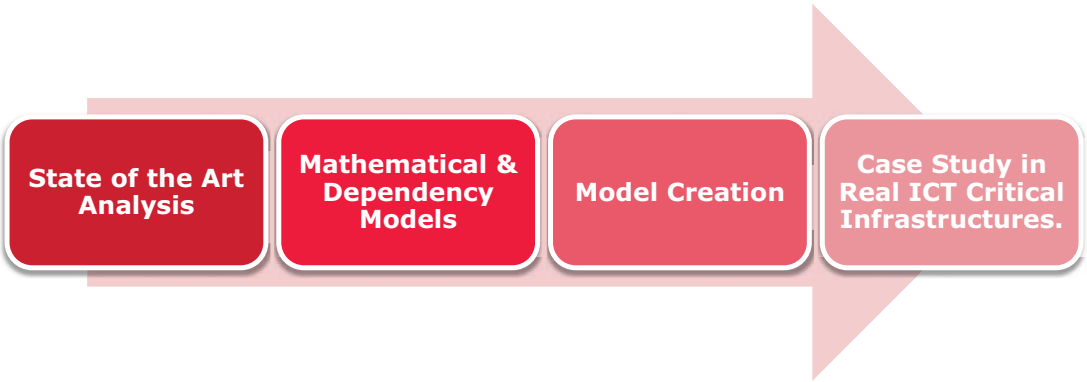
UNCLASSIFIED INFORMATION

INNOVATING SOLUTIONS

PLANNING

- 18 Months: 1st July 2012 – 31st December 2013

- Focused and applied research
- Validate results in real infrastructures



CISIM – 2nd CIPS WORKSHOP

EXPECTED RESULTS

INNOVATING SOLUTIONS

EXPECTED RESULTS

- Objectives targeted:

1. Forecasting resilience of large infrastructures (>=1000 elements) in less than 6 hours

2. Forecast interdependable ICT critical infrastructures resilience

3. Confidentiality and integrity forecasting approach

Proceedings of the CIPS II Workshop

Online identification of Failure and Attack on interdependent Critical Infrastructures

Roberto Setola

Universita degli Studi Roma3

email: r.setola@unicampus.it

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme
European Commission - Directorate-General Home Affairs

FACIES

online identification of Failure and Attack on interdependent Critical InfrastructurES

Start: 1st September, 2012
End: 28th February, 2014

Laboratorio Sistemi Complessi e Sicurezza

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA

Associated partner:

AIIC

uma RadioLabs University of Cyprus

FACIES partners

University Campus Bio-Medico of Rome (Italy)
Complex Systems and Security Lab –COSERITY Lab

University of Malaga (Spain)
Network, Information and Computer Security Lab – NICS Lab

RadioLabs (Italy)
Consortium Universities-Companies – RadioCommunication Laboratories

University of Cyprus (Cyprus)
KIOS Research Center for Intelligent Systems and Networks

Associated partner:

AIIC (Italy)
Italian Association of Critical Infrastructures' experts

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

FACIES

Interdependency Modelling

Fault detection

cybersecurity

Data Fusion

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

Objective of the project

The objective of **FACIES** project is to define cooperation strategies for automatic detection of failures and attacks.

The solution has to be achieved in a **decentralized** and peer-to-peer perspective where only partial and not sensible data are shared among the different subjects.

A particular attention will be posed on cyber threats and **stealth** attacks.

The project aims to illustrate the feasibility on a (hydric) reference scenario implemented via ***testbed***.

Motivation for fault diagnosis

- Critical Infrastructures are sophisticated system dispersed on large geographical area with a large number of components and subparts
- Huge data of different characteristics (in time and space)
- Advanced data processing and automated decision making

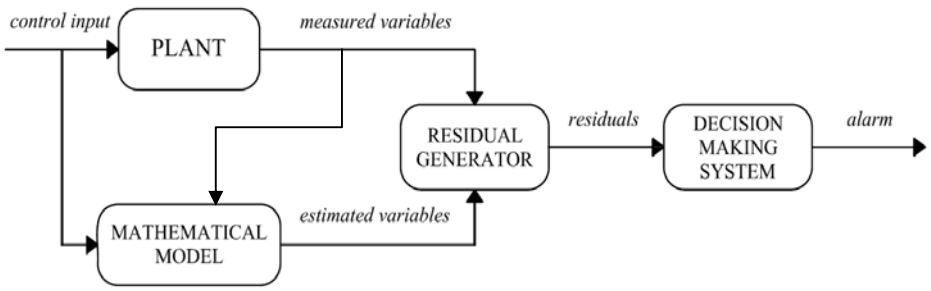
- **However, data may be faulty, inconsistent or missing (nonsense data)**
- **Faulty data may result in wrong decisions or escalation to a failure**

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

FACIES

FAULT DETECTION

Are a set of techniques devoted to automatically identify **anomaly behavior** (e.g. fault) into a process system



The main idea is those to constantly compare the output of the actual system (*the plant*) with those foreseen by a mathematical/simulated model of the system (*the estimator*) . The presence of large discrepancies indicate the existence of a fault

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

FACIES

FAULT DETECTION

- **Fault detection** (There has been a fault)
- **Fault isolation** (there has been a fault of a specific type)
- **Fault accomodation** (how to reconfigure the system to be trasparent w.r.t the fault)

To early detect a fault and prevent "small" fault events from escalating into a major failure

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

FACIES

Detectability Conditions

- Generally only a very limited set of measure are available
- Our knowledge (mathematical model) of the process is not perfect

- In order to be recognise a «fault» has to detectable (i.e. have to be observable from our measuremets)

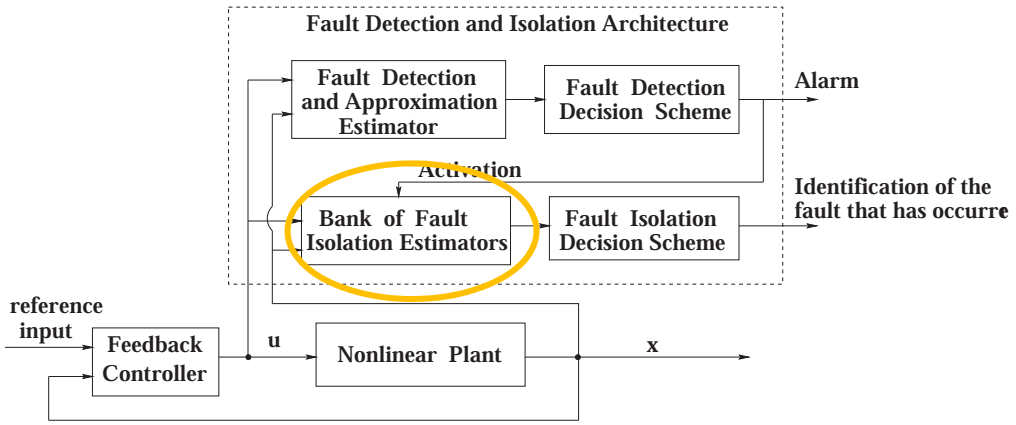
$$\left| \int_{t_1}^{t_2} e^{-\lambda_i^0 (t_2 - \tau)} \left(1 - e^{-\alpha_i (\tau - T_0)}\right) f_i(x(\tau), u(\tau)) d\tau \right| > \frac{2\bar{\eta}_i}{\lambda_i^0},$$

There is always a tradeoff between the detection capabilities (# of not recognized event – positive false) and the robustness of the approach (# of erroneous alarm – false positive)

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

Fault Isolation schema

➢ We need to have a model of the “modus-operandi” of the fault in order to discriminate it



UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

Moving from system to infrastructure

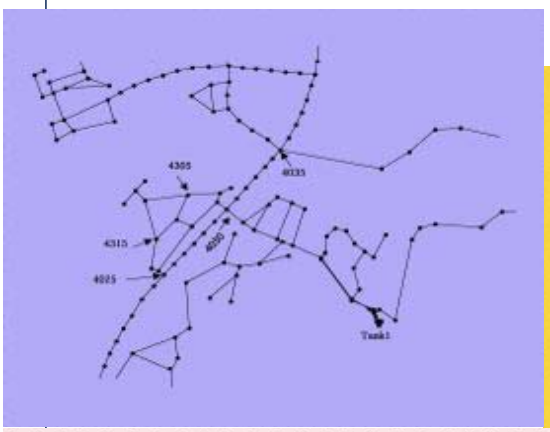
- Local Faults
- Distributed Faults
- Distributed Faults with Overlapping Signature
- Propagating Faults

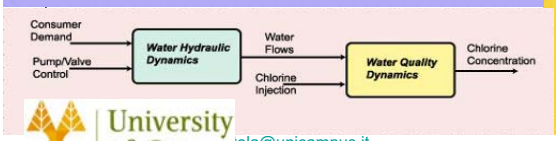
Types of FAULT ISOLATION:
- identify the type of fault that has occurred
- identify the physical location of the fault

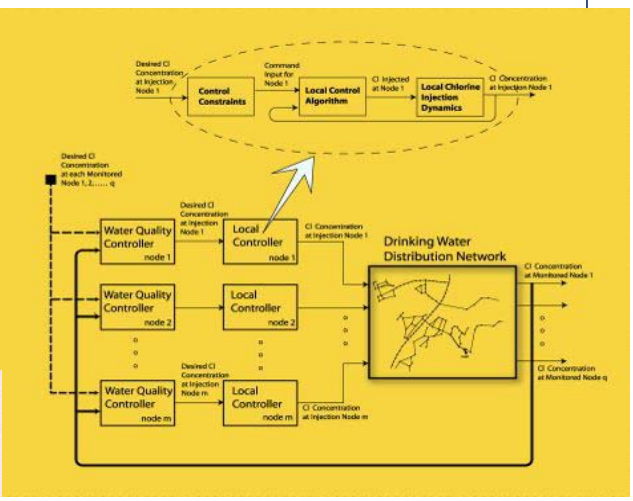
UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

Example: Water Distribution Networks

Objective: control the spatio-temporal distribution of drinking water disinfectant throughout the network by the injection of appropriate amount of disinfectant at suitably chosen actuator locations.





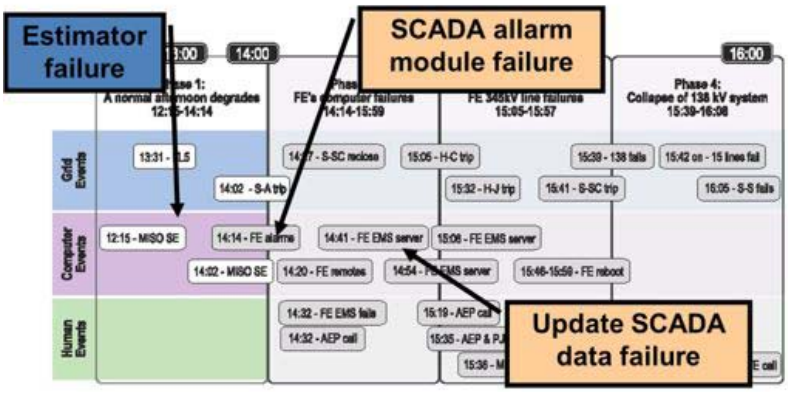


University of Cyprus
:ola@unicampus.it

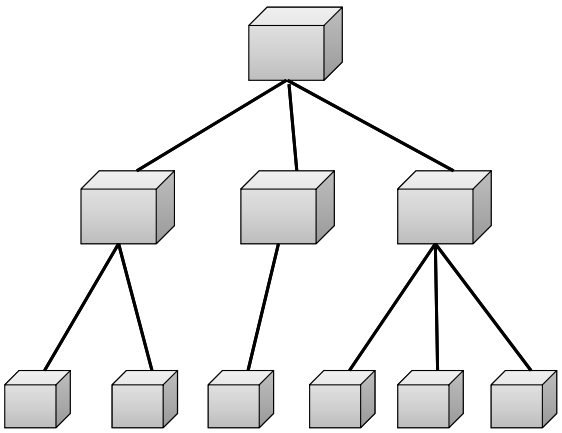
FAULT DETECTION

Quite all the Critical Infrastructure has such type of system (labbed in different way as estimator, bada data detector, etc.) to help operators to better monitoring their system

2003 – US & Canada blackout



The comlpexity of the problem is increasing

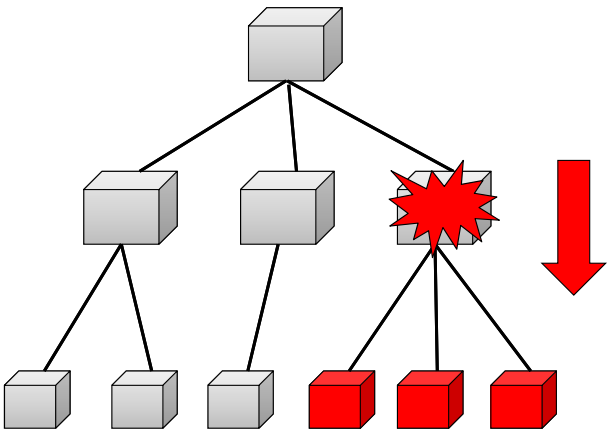


Classical infrastructure have been designed as tree like structure

A fault into a component/subsystem will affect downstairs component (directional propagation of the fault)

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

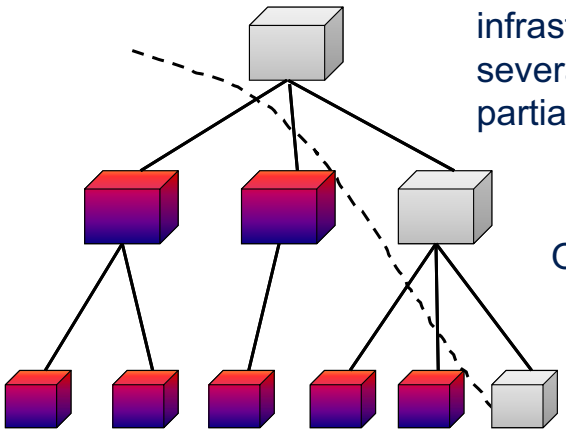
The comlpexity of the problem is increasing



I can easily identify the “root” of the failure and the corresponding cause-effect phenomena

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

The comlpexity of the problem is increasing



Due to deregulation any infrastructure is now managed by several operators each one has a partial view of the whole process

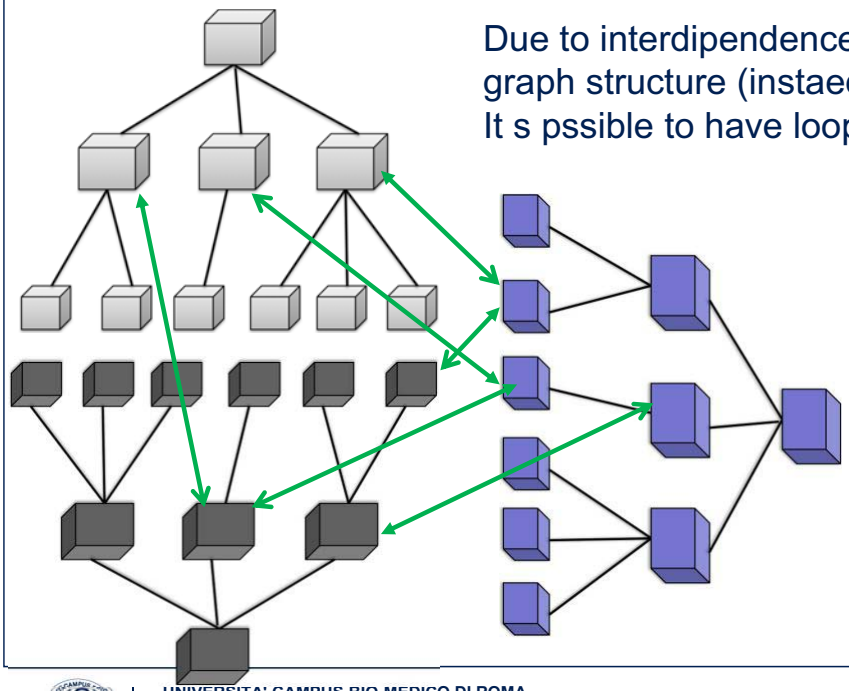
Operator #1

Operator #2

No one has a complete picture of the whole system

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

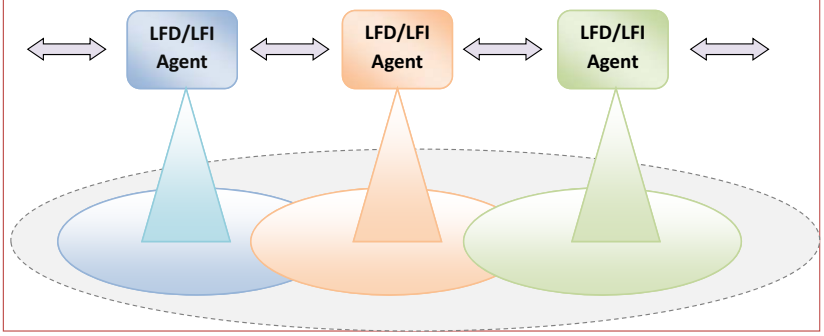
The comlpexity of the problem is increasing



Due to interdipendence, we have a graph structure (instaed of a tree). It s pssible to have loop

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

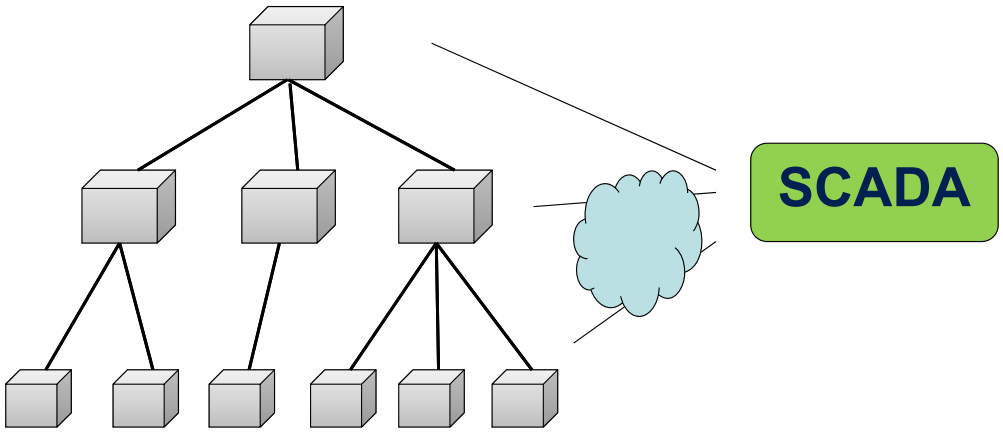
Each operator can monitor its own domain, but he have to accommodate for phenomena that are generated outside



UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

FACIES

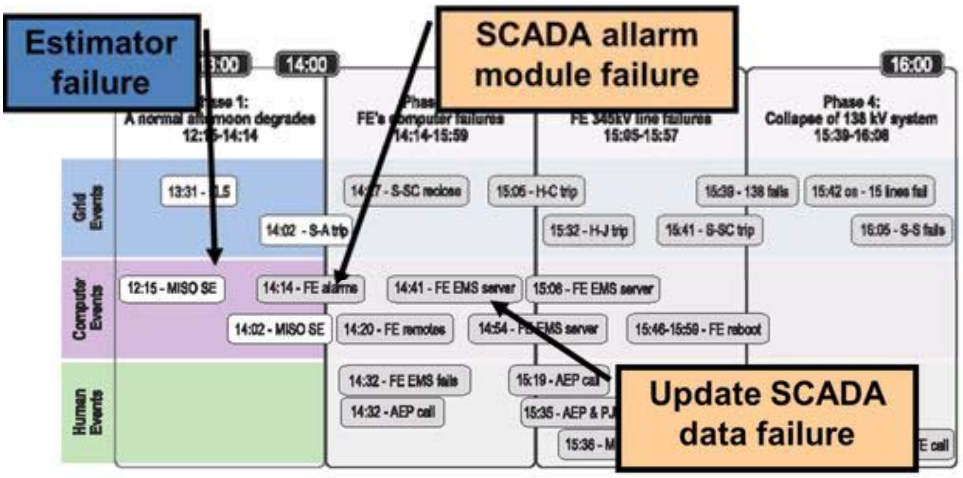
The comlpexity of the problem is increasing



All data have to be collected via ICT (also internet), fault may happen also in the communication link and/or SW and one has to consider also cyber attack

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

2003 – US & Canada blackout



UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

The cyber threat

- ✓ A DDoS attack can block the communication (e.g. slammer worm)
- ✓ A virus/worm may block the server (e.g. slammer worm)
- ✓ A virus/worm may modify the normal behaviour of the process control (e.g. stuxnet)
- ✓ An hacker can introduce into the system and modify the data (data corruption)

But also

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

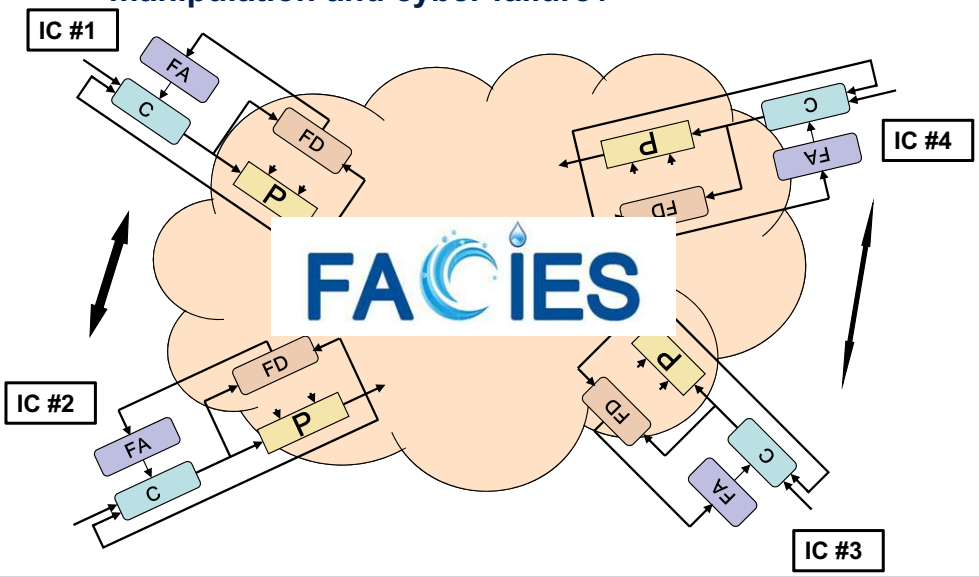
The cyber threat 2

The cyber action can be targeted to the fault detection system with the aim of:

- **Induce false alarms.** It is more easy to inject anomalous data and force the system automatically adopts emergency procedure (e.g. shout-down), rather than be able to malicious introduce a dangerous sequence of command
- **Masking a cyber/phisical attack**, i.e. make the attach undetectable by the fault detection system (**stealth attack**)

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

How identify failures/attacks having a partial and limited vision of the process in the presence of interdepenencies and taking into account also the possible cyber-data manipulation and cyber failure?



UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

FACIES

To roadmap (on working .)

1. Review of the most suited/innovative technologies for fault detection/isolation in order to valuate their applicability into a distributed framework scenario and to test their effectiveness/weakness w.r.t. malicious attack

2. Review of the most relevant methodologies to improve situation awareness (data fusion) applicable in a decentralised scenario

3. Review of the most cyber recent attack against critical infrastructure's monitoring system with a specific focus on those action performed to avoid to trigger alarms (i.e. stealth attack) in order to identify conditions/strategies able to hide the attack

To roadmap (.to be done)

5. Development of (innovative) fault detection procedures specifically designed for CI

6. Implement and validate w.r.t. a realisitc test bed scenario

4. Realise a cyber/physical test bed to be used for validation phase

(*but also to be shared as an ERNCIP facility*)

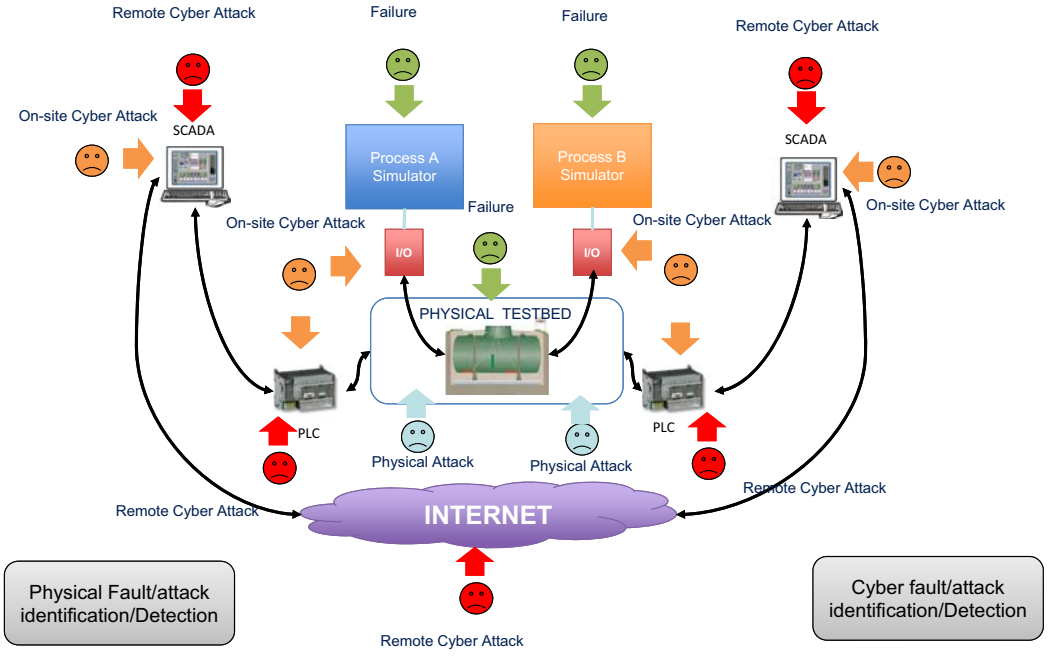
Testbed requirements

• The testbed will reproduce the main characteristics of a critical infrastructure, and, in particular, considering the effects of **interdipendencies**.

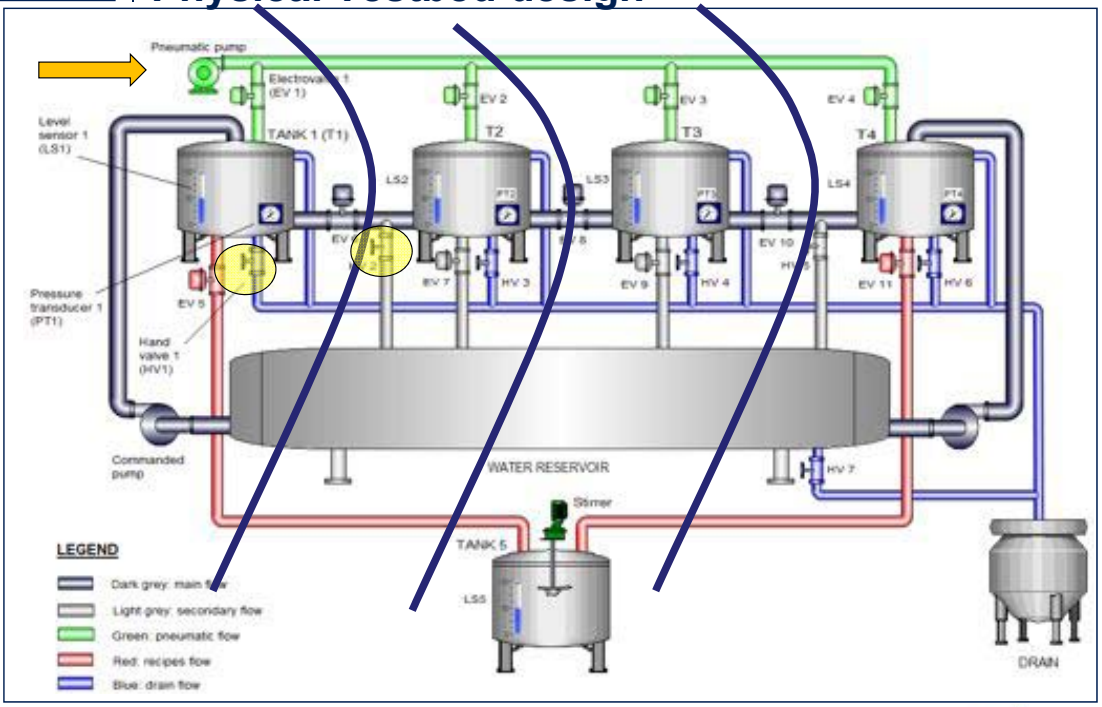
• The hardware testbed will be interfaced on one side with at least two simulated processes, and on the other side with at least two different controllers (PLC/SCADA System) to test the different detection techniques.

• The software testbed will allow the simulation of different scenarios, in which the infrastructure normal functioning is compromised.

Testbed



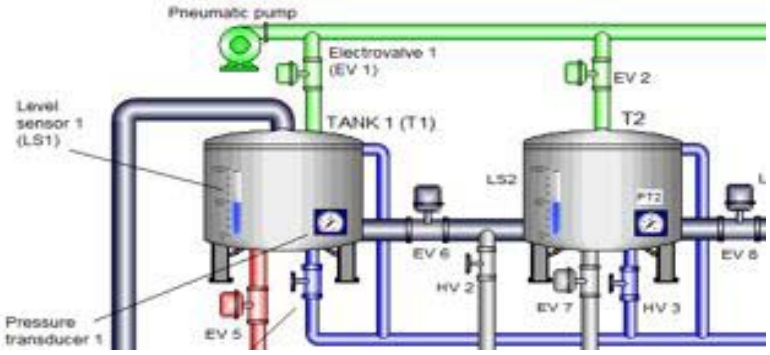
Physical Testbed design



UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

FACIES

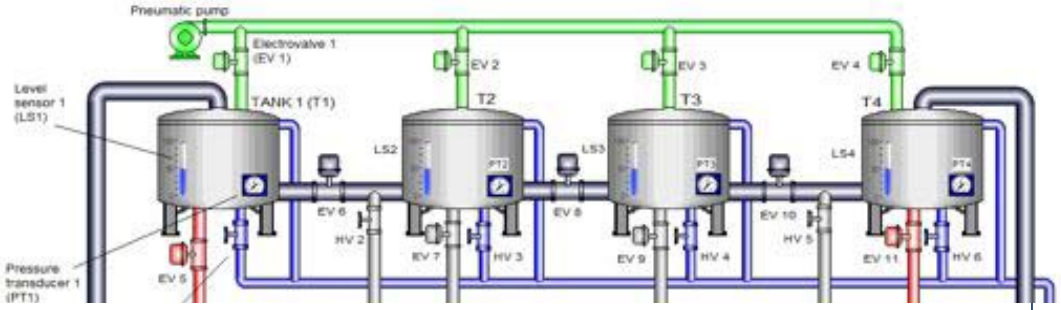
Simulated Scenarios – Leakages and pressure drops



Holes in tanks or pipes may cause leakages and pressure drops, which can be detected monitoring **sensors state**, e.g. comparing level increase in tank 2 and output water from tank 1, depending on level sensor state 1 and pressure value in tank 1. Changing the values of these variables it is possible to reproduce such situations, e.g. opening HV 2 it may represent a leakage between T1 and T2.

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

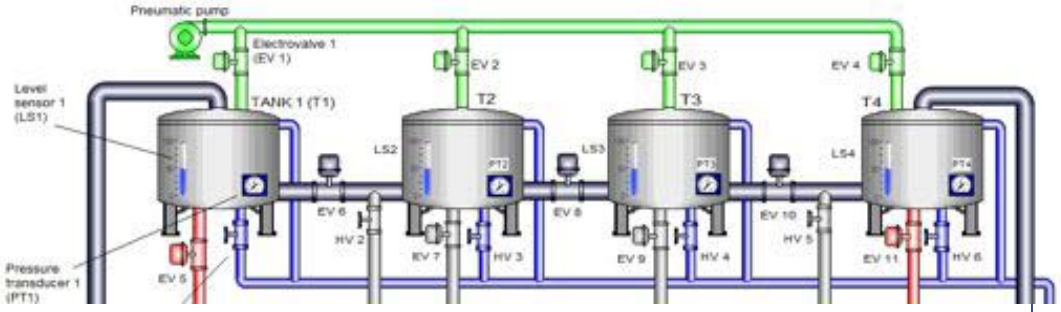
Simulated Scenarios – Increasing tank pressure



Tank pressure is measured by a pressure transducer, one for each tank. Varying EV1, EV2, EV3 and EV4 inlet, it is possible to simulate a scenario in which tank pressure increases, exeeding threshold values.

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

Simulated scenarios – Sensor attacks



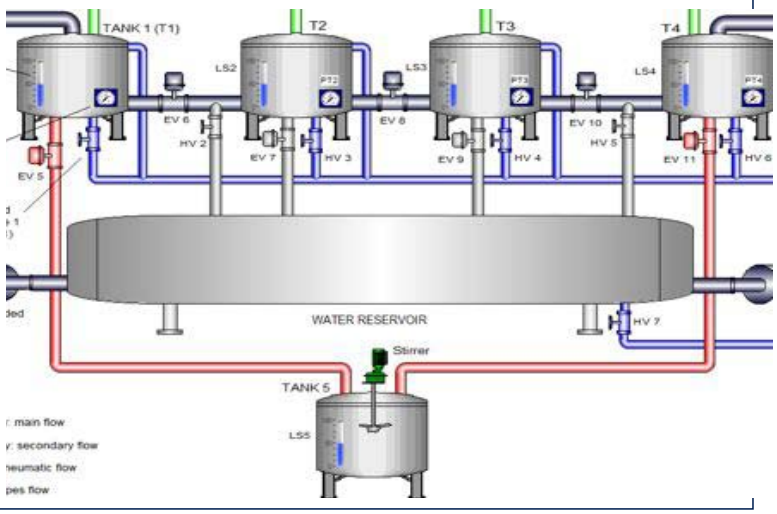
Sensors reliability is of the utmost importance in control systems. Bad data caused by faults or physical/cyber manipulation can lead to unpredictable and sometimes dangerous consequences.

For example a wrong pressure value may cause physical damage to many system components, such as valves, sensors and pumps, or become dangerous for peolpe around.

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

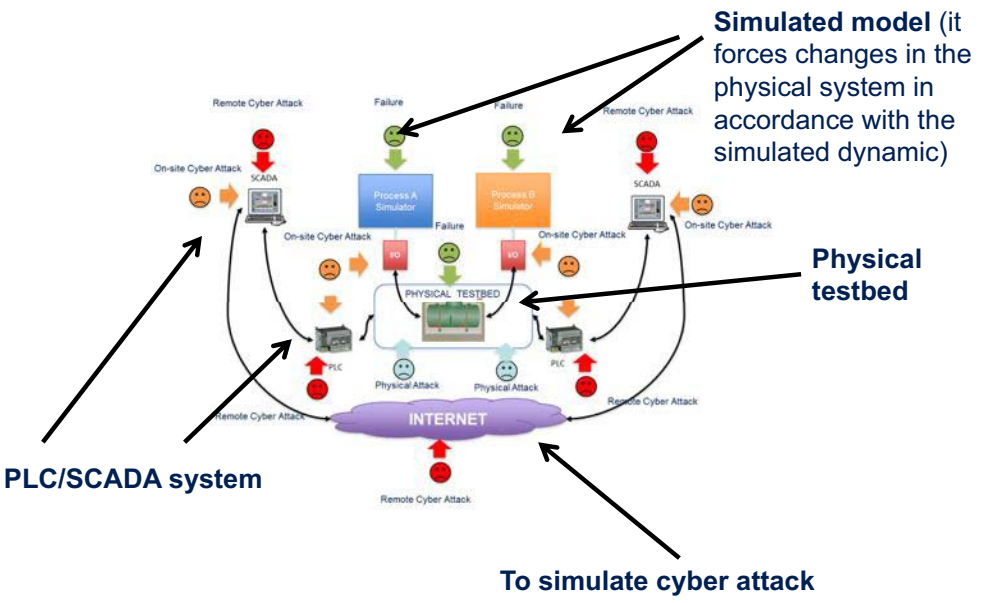
Simulated Scenarios – Wrong percentages of chemicals in recipes

Chemicals percentage piped to tank 5 depend on EV 5 and EV 11 inlets. Varying these variables it is possible to modify expected fraction of chemicals in the considered recipe.



UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

Physica testbed is a part of FACIES testbed



UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it

Simulated scenarios

Some test scenarios may also allow to:

- **Consider physical attack to sensor/actuator**
- **Leakages and pressure drops**
- **Increasing tank pressure**
- **Sensor attacks**
- **Wrong percentages of chemicals in recipes**

Thank you for your attention!

FACIES

online identification of Failure and Attack on interdependent Critical InfrastructurES

Website: http://facies.dia.uniroma3.it

Roberto Setola
r.setola@unicampus.it

UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
r.setola@unicampus.it
FACIES

Proceedings of the CIPS II Workshop

Threat-Vulnerability Path Identification for Critical Infrastructures Compilation of a comprehensive all-hazards catalogue for critical infrastructure

Paolo Trucco

Politecnico di Milano

email: paolo.trucco@polimi.it

THREVI^2 Project

Compilation of a comprehensive and dynamic all-hazards catalogue for critical infrastructures

Prof. Paolo Trucco
Department of Management, Economics
and Industrial Engineering
Politecnico di Milano

Ispra, 22-23 November 2012

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS
Directorate A : Internal Security

THREVI^2 consortium

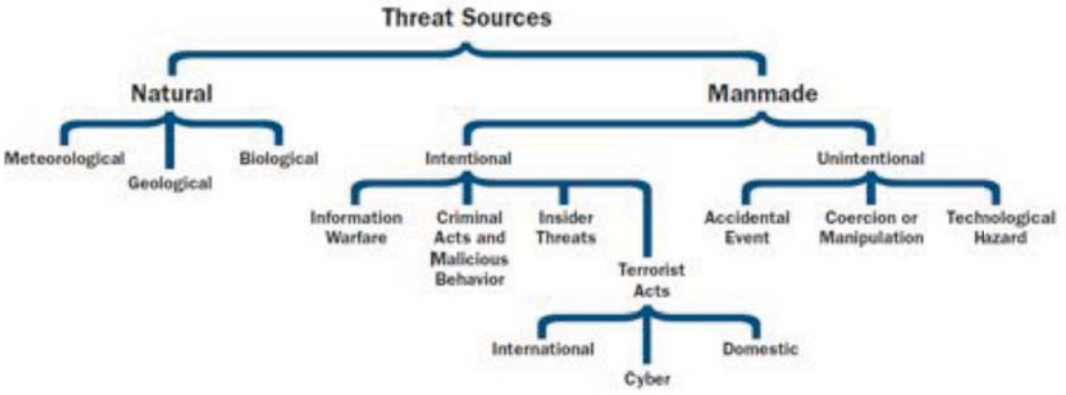
Threat - Vulnerability Path Identification for Critical Infrastructures

- NIER Ingegneria S.p.A (NIER) - Coordinator
- RGS S.r.l., Risk Governance Solutions (RGS)
- Politecnico di Milano, Department of Management, Economics and Industrial Engineering (POLIMI)
- Università Campus Bio-Medico di Roma - Faculty of Engineering (UCBM)

THREVI^2 project rationale

Threat - Vulnerability Path Identification for Critical Infrastructures

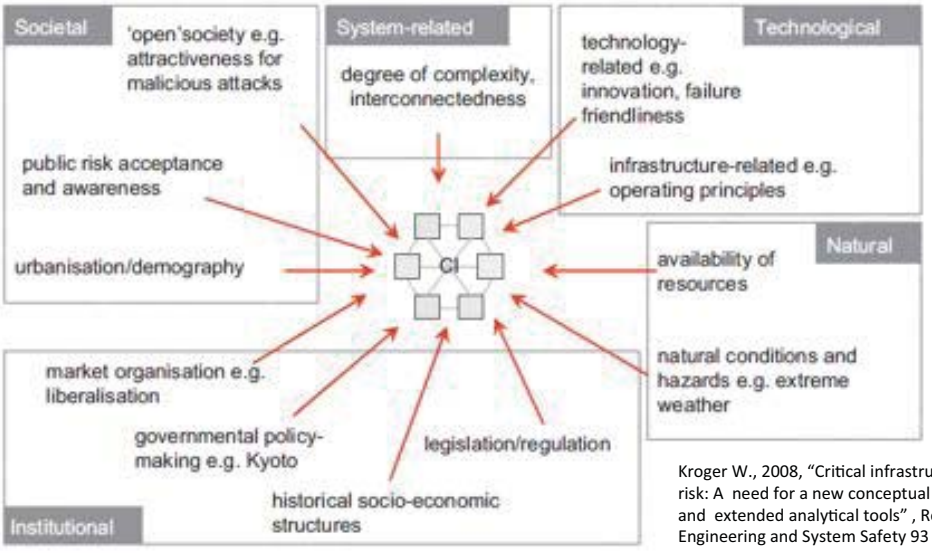
- CI are exposed to different types of hazards and threats



THREVI^2 project rationale

Threat - Vulnerability Path Identification for Critical Infrastructures

- … but several other factors influence their complex response



Kroger W., 2008, "Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools" , Reliability Engineering and System Safety 93 (2008)

THREVI² project rationale

Threat - Vulnerability Path Identification for Critical Infrastructures

- **Threat identification** and assessment is relevant to:
  - CI systems and assets identification and designation
  - Assess potential vulnerabilities and impacts
  - Define adequate prevention or protection countermeasures
- **Comprehensiveness** and **consistency** of information on threats are crucial for:
  - Complete reference knowledge
  - Common understanding of potential scenarios
  - Comparable analyses

THREVI² project rationale

Threat - Vulnerability Path Identification for Critical Infrastructures

End users are facing some key issues:

- How to practically apply an all hazard approach to CI systems ?
- How to account for and characterise main vulnerabilities of CI systems as well as domino effects between interdependent CIs?
- How to identify the types of potential impacts and consequences with regard to a wide spectrum of targets?

THREVI² objectives

Threat - Vulnerability Path Identification for Critical Infrastructures

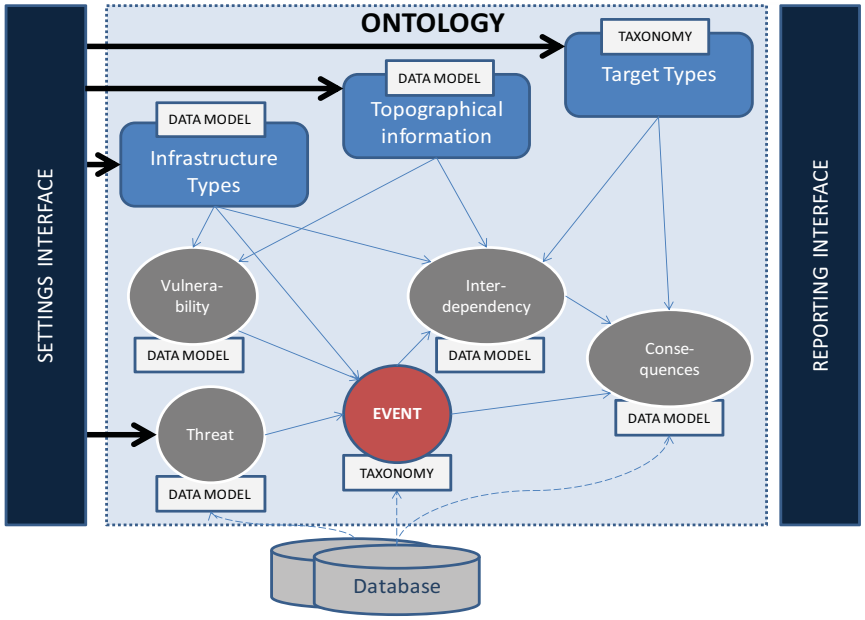
- To support **scenario definition** within CIP programmes
  - Enhanced knowledge on hazards and threats affecting CIs systems and related vulnerabilities.
  - Improved CIs designation process and related risk assessment

- **PATHFINDER Tool**, a relational database to screen relevant threat-consequence mechanisms for CI systems and assets.

  "*To create a Database (DB) linking the relationships between all the hazards threatening CIs and the vulnerability of the CIs' systems or components; the query of the DB will allow the end-users (CIP Authorities and operators) to identify relevant scenarios, according to their own priorities and criteria*"

THREVI² - PATHFINDER Tool

Threat - Vulnerability Path Identification for Critical Infrastructures



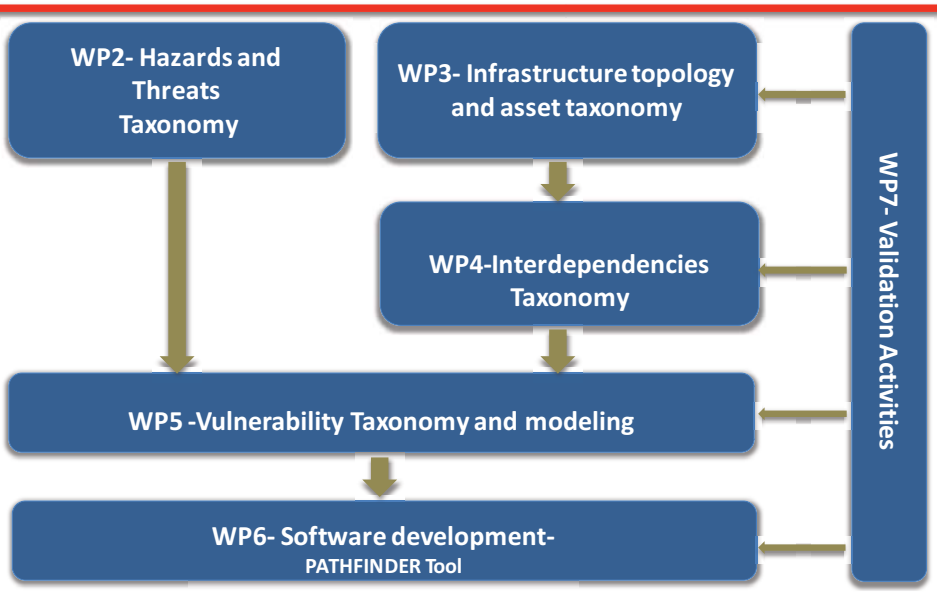
Intended beneficiaries and applications

Threat - Vulnerability Path Identification for Critical Infrastructures

	Public Authorities	CI Operators	CI Customers
CIP Governance and PPP implementation	▪ CI designation ▪ CI impact assessment	▪ Vital node analysis ▪ Information sharing	
Land use planning	▪ CI impact assessment ▪ Societal risk assessment		
CI systems design and operations	▪ Design review ▪ Certification ▪ Auditing	▪ Resilience engineering	▪ Resilience engineering
Emergency Planning	▪ Plan design and audit ▪ Training and exercises	▪ Business continuity planning	▪ Business continuity planning

THREVI^2 Work Breakdown Structure

Threat - Vulnerability Path Identification for Critical Infrastructures



Duration: 24 months from 01 September 2012

Request for contributions and involvement

Threat - Vulnerability Path Identification for Critical Infrastructures

- Sources for the definition of the Infrastructure Topology and Asset Taxonomy (ITAT)

		Regulatory	Scientific	Technical
Energy Infrastructure	**Electricity**			
	Gas			
	Oil			
TLC Infrastructure	**Fixed**			
	Mobile			
Transportation Infrastructure	**Air**			
	Inland Water Ways			
	Ocean and Short-Sea Shipping and Ports			
	Rail			
	Road			
Water Infrastructure	**Service Water**			
	Waste Water			
General	**General**			

Request for contributions and involvement

Threat - Vulnerability Path Identification for Critical Infrastructures

- THREVI^2 validation
  - **Validation of Ontologies**
    involvement of CI experts from public authorities and safety managers from Operators. Two steps procedure:
    1. experts will be provided with a preliminary version of the ontology and with a document describing the rationale; on the basis of the received feedbacks the ontologies will be finalised;
    2. experts will be provided with the final version of the ontologies along with a template for formally reviewing the work.
  - **Validation of the Software Tool**
    identification of a couple of pilot applications in some Member States or European Regions, where reference experts will be provided with the final version of the PATHFINDER tool for a test application

Conclusions

- THREVI^2 will harmonise and integrate all the available knowledge for the characterisation of threats, vulnerabilities and interdependencies of CIs systems
- THREVI^2 will provide CI experts with a dynamic catalogue - the PATHFINDER Tool – to support scenario setting within a wide spectrum of applications
- THREVI^2 will implement a consistent validation process involving European public bodies and operators

Threat - Vulnerability Path Identification for Critical Infrastructures

Thank you!

Prof. Paolo Trucco
Dept. Management, Economics and Industrial Engineering
Via Lambruschini 4/b - building 26/B - 20156 Milan (Italy)

office: +39 02 2399 4053
fax: +39 02 2399 4067
e-mail: paolo.trucco@polimi.it
website: http://www.ssrm.polimi.it/

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS
Directorate A : Internal Security

Proceedings of the CIPS II Workshop

Risk Assessment and Development of Protection Capacity for Critical Infrastructures due to Aircraft Attack

Fritz-Otto Henkel

Wölfel Beratende Ingenieure

email: henkel@woelfel.de

RiskProtect CI

Fritz-Otto Henkel

Wölfel Beratende Ingenieure
Max-Planck-Straße 15
97204 Höchberg/Germany

Fon +49-931-49708-0
henkel@woelfel.de
Web www.woelfel.de

RiskProtect CI

Project Information:

Call:	CIPS 2010 II **Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks**
Project Title:	**Risk Assessment and Development of Protection Capacity for Critical Infrastructures due to Aircraft Attack**
Acronym:	RiskProtec CI
Contract N°:	HOME/2010/CIPS/AG/045
Project Start:	1st January 2012
Project End:	31st December 2013

RiskProtect CI

- Applicant: Wölfel Beratende Ingenieure GmbH + Co. KG, Germany
- Partners
  - Risk Engineering Ltd, Bulgaria, (REL)
  - Bulgarian Academy of Science, (NIGGG)
  - Bulgarian Atomic Forum, (Bulatom)

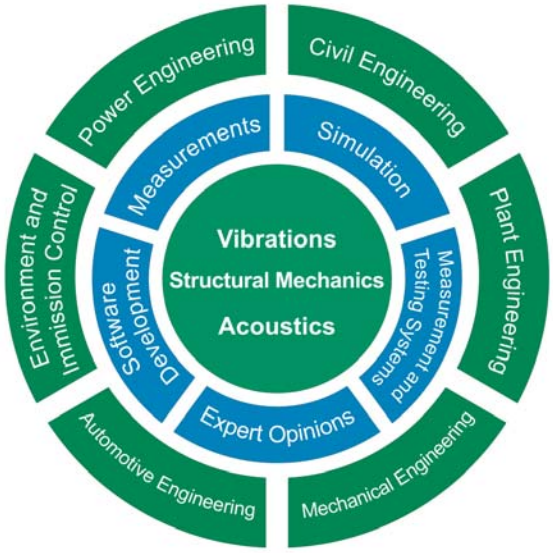
- Eligible costs: 835.679,00 €
- Grant: 584.975,30 €

HITech, Max-Planck-Straße, Höchberg

1971	Foundation of Woelfel Beratende Ingenieure Residence: Hoechberg near Wuerzburg, Germany
1985	Foundation of Woelfel Meßsysteme · Software
1986	Prof. Dr.-Ing. H. P. Woelfel, TU Darmstadt, Mechanical Dynamics Legal form GmbH + Co. KG, Emeritus 2006
2000	Relocation HITech
2009	Shareholder of Micromega S.A.

Experts for Vibrations, structural dynamics, acoustics

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion



- Wölfel is an European engineering company in structural dynamics
- More than 800 projects in Europe, Asia and America per year

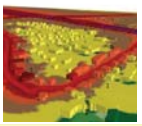
Business Units

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

Nuclear

Plant Engineering

Civil Engineering, Plastics



Acoustics, Building Physics

Vibrations

Structural Dynamics

Earthquake

Mechanical Dynamics

Automotive

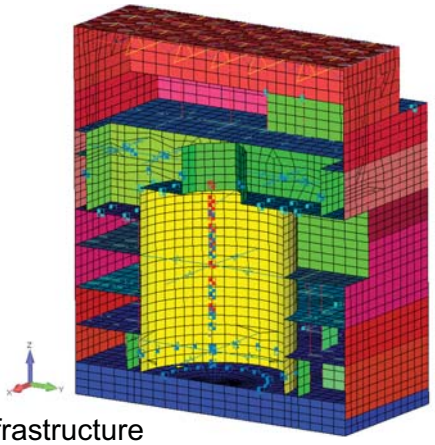
Biomechanics, Seating Comfort

Wind Energy

Nuclear and Critical Infrastructure

Load cases WBI is experienced in industrial projects as well as in R+D projects:

- Earthquake
- Airplane crash
- Pressure waves



Critical Infrastructure WBI has dealt with

- Buildings
- Plants and components
- Control and communication systems

Know-how of WBI: Protection of critical infrastructure

- Vulnerability
- Protection concepts

R&D

Wölfel

RISK ENGINEERING LTD.
Reliability, Safety and Management
Engineering and Software Development Services

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

BUSINESSES

Nuclear Energy

- Safety Management
- Operational Improvement
- Rad-Waste and Spent Fuel Management
- New build

Conventional Energy & Energy-saving Technologies

- Thermal power plants
- Cogeneration facilities
- Energy efficiency

Renewable Energy

- Hydro power plants
- Photovoltaic plants
- Wind parks

Structure of Bulgarian Atomic Forum

Overview

Partners

Tasks

Risk Assessment

Analysis

Conclusion

- The membership of Bulatom is made up of 94 companies, which are performing business in the nuclear field in Bulgaria (mainly Kozloduy NPP, Belene NPP, Nuclear Research Reactor in Sofia and other).
- Bulatom is a member of Foratom – the association of the European nuclear industry.
- Bulatom is established as organization, which has to represent the interests of the Bulgarian nuclear industry. In pursuing this goal, Bulgarian Atomic Forum aims to participate fully in Europe's energy debate and to make the voice of the Bulgarian nuclear industry heard in the discussions about the EU's energy future.

RiskProtec CI
Technical Work 1

Overview

Partners

Tasks

Risk Assessment

Analysis

Conclusion

Responsibility for Structures:

- REL: Russian NPPs,
- REL, NIGGG: dams
- WBI: German NPPs

Development of a methodology for the risk assessment of NPP and dams

- General concept of risk assessment
- Assessment method for NPP structures
- State of the art of computational methods for aircraft impact
- Further development of methods
  - FEM Models of the structures
  - FEM Models of planes
  - Material models for crash analysis

Review of the hazardous CI structures

- Lists of types of NPPs and dams
- Classification of NPPs and Dams with regard to airplane crash

RiskProtec CI
Technical Work 2

Overview

Partners

Tasks

Risk Assessment

Analysis

Conclusion

Analysis of vulnerability of NPPs and dams

- Basis for protection capacity against airplane crash

Development of protection capacity against airplane crash of commercial passenger planes

- high performance concrete
- development of an additional shelter layers
- additional obstacles in flight direction to structure

Proof of different protection concepts by computational analysis

No investigation of

- Fire balls
- Safety related components within the structures

Dissemination Activities
Conferences and Workshops

Overview

Partners

Tasks

Risk Assessment

Analysis

Conclusion

Participation in and contributions to international conferences

- BULATOM 2012, 30th May – 1st June, 2012, Varna, at least 3 contributions
- BULATOM 2013, end of May 2013, Varna, at least 3 contributions
- SMIRT 22, 18. – 23,. August 2013, San Francisco, at least 3 contributions

Specific Workshops in parallel to Bulatom 2012 and 2013

- RiskProtec CI Workshop at BULATOM 2012, 1st June, 2012, Varna
- RiskProtec CI Workshop at BULATOM 2013, end of May 2013, Varna

New !

Contribution to IAEA Safety report series “Safety Assessment of NPP Structures against Human induced Events”

Deliverables

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

- D 1: report on method
- D 2: list of vulnerable CI (dams, NPPs) and classification due to type and protection class report
- D 3: protection capacity needed, report
- D 4: protection capacity for CI including publications
- D 5: Participation in and contributions to international conferences
  - SMIRT 22, 2013, USA, at least 3 contributions
  - Bulatom 2012, Bulgaria, at least 3 contributions
  - Bulatom 2013, Bulgaria, at least 3 contributions
- D 6: specific Workshops in parallel to Bulatom 2012 and 2013

Milestones

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

M 1 31st August 2012:
- methodology for the risk assessment of NPP and dams is developed
- D1 is available

M 2 31st August 2013:
- list of vulnerable CI and classification due to type and protection class is compiled
- D2 is available

M 3 31st December 2013:
- protection capacity against crash with commercial aircrafts is developed
- D3 and D 4 is available

General Concept of Risk Assessment

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

- **Risk = Frequency of occurrence x Extent of damage**

- Risk = H x R x C
- H = Frequency of occurrence (Hazard)
- R = Conditional probability of failure (Resistance)
- C = Extend of damage as a result of a Consequence analysis

- Theory developed in earthquake engineering
- Hazard quantification not in force for malevolent human acts and terroristic attacks

- Attack with maximum probable parameters: mass and velocity

Variants of analysis of airplane crash

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

State of the art, developed till 1989

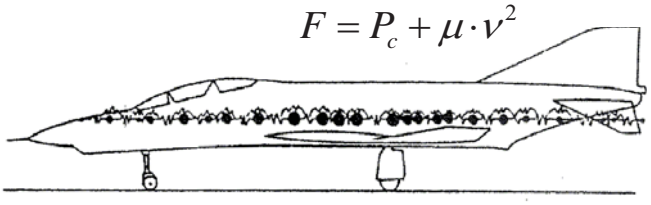
State of the art, developed since 2001

- Load definition
- Model of Airplane and NPP
- Stability of structure

History of F-t-Function

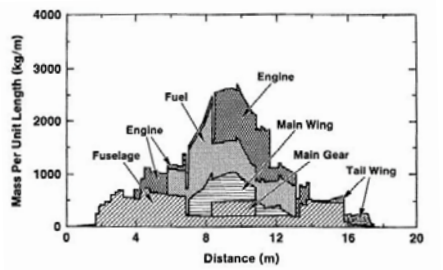
- Initial point for computing the F-t-Function is Riera's publication* of 1968 describing the aircraft simplified with a mass-spring-system, hitting a rigid target
- The analytical procedure is based in principle on a simple momentum equation, where the behaviour is defined by two parts

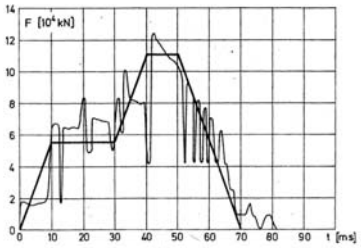
$$F = P_c + \mu \cdot v^2$$



P_c = crushing force
μ = mass flow
v = velocity

- For practical use the F-t Function was smoothed





Riera: ‚On the Stress Analysis of Structures … ',Nuclear Engineering and Design, 1968

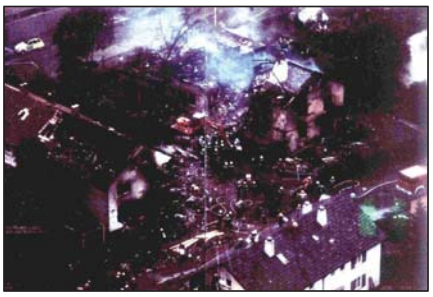
R&D

History of F-t-Function

Wölfel

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

- First application scenarios of F-t-function within structural analysis appeared in Germany in the 70'ies due to of two facts:
  - Geopolitical situation within iron curtain between East and West - high number of military jets located near the boarder
  - Problems within setup, handling and service of Starfighter caused several crashes with dramatic damages

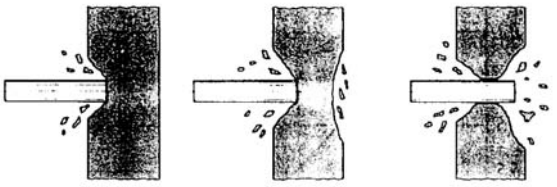


Crash of military jet in a urban residential district in Germany

Missile Impact

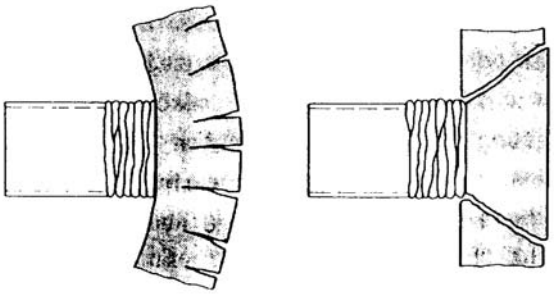
- There are two main types for the impact of missiles, depending on the stiffness relation between missile and target

Hard Impact



spallation penetration scabbing perforation

Soft Impact



overall target response punch type shear failure

Aircraft Crash – Sandia

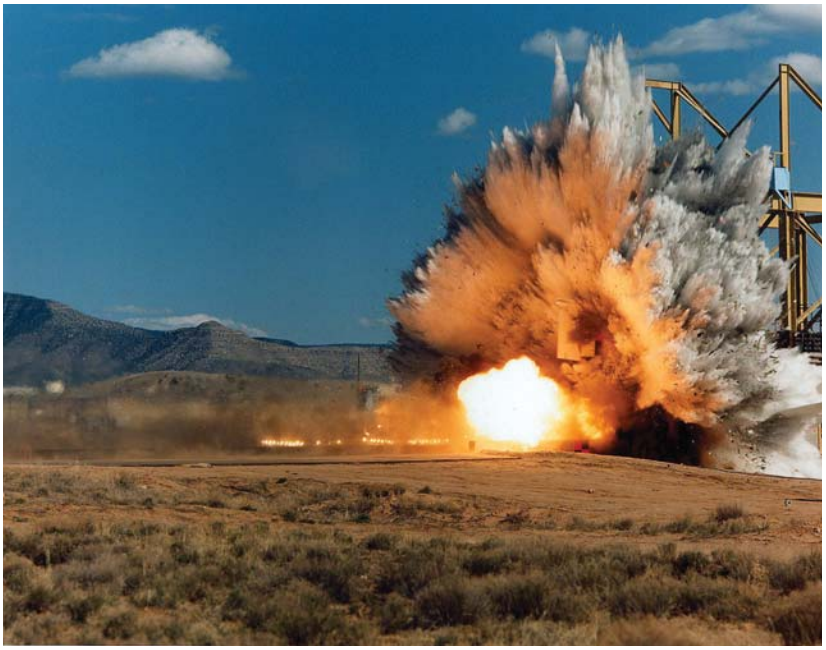
- In 1988 a crash of a military jet (Phantom F4) on a concrete slab was conducted at Sandia National Lab, Albuquerque, New Mexiko, USA
- The final velocity was 215 m/s, accelerated by rocket sled facility

Aircraft Crash – Sandia

Aircraft Crash – Sandia

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

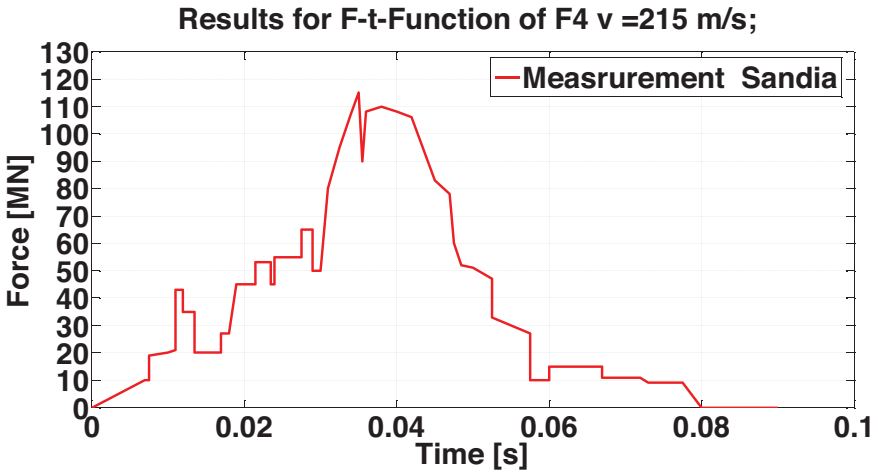
Aircraft Crash – Sandia



Aircraft Crash – Sandia

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

- The goal was the experimental determination of the F-t-function
- Accordingly the concrete wall was designed to be almost rigid, thickness 3.66 m, area 7m², weight 469 t

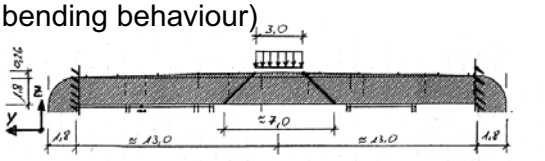


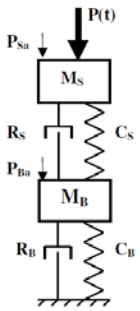
Analysis Types

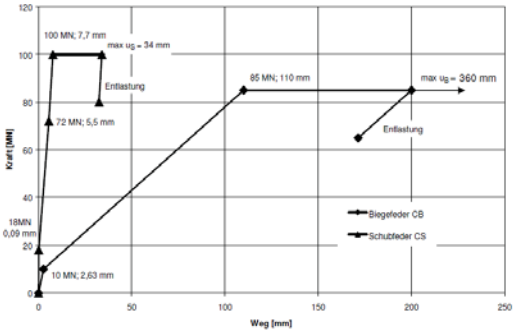
- Local analysis
  - perforation (using empirical equations)
  - local damage (shear, bending, punching)
- Global analysis
  - stability (sliding, overturning)s
  - strength (design of stiffening elements)
  - displacements (contact to neighbouring structures)
- Vibration analysis
  - floor response spectra
  - vibration of secondary structures (components)
- Fire scenarios

Local Analysis - Damage

- Simplified Mass-Spring-Damper-Model with two 2 DOF (shear and bending behaviour)

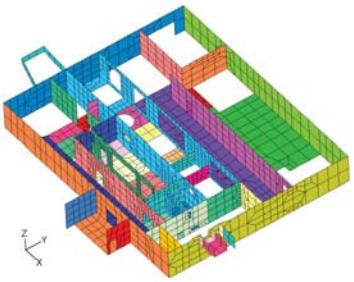




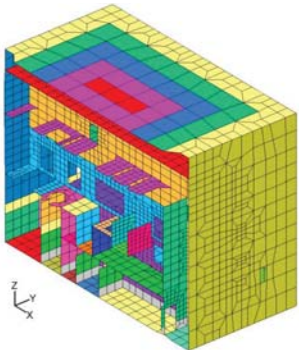


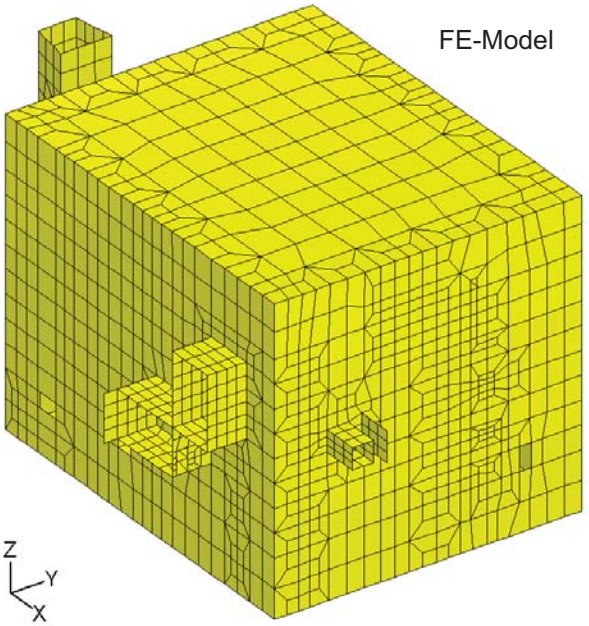
- Input data is e.g. F-t-function out of test or Riera approach

Global Analysis – FE-Method



Sections FE-Model





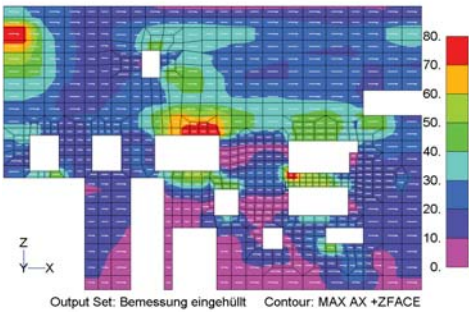
R&D

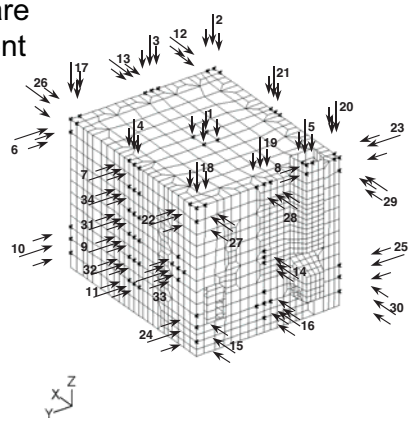
Global Analysis – FE-Method

Wölfel

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

- As load case the F-t-function is used. The computation can be carried out as modal analysis based on the eigenfrequencies and –modes or using a direct integration scheme in the time domain
- Reflecting real scenarios all possible impact areas are investigated
- Final goal of the simulation is the computation of internal forces, displacement and accelerations, which are used for reinforcement design, component analysis…





Motivation for new methods

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

- The impact of a military plane on a nuclear power plant has been a standard load case in Germany since the 1970ies
- Due to limited numerical capabilities the analysis has been divided (decoupled) into two steps:
  - Definition of the F-t-Function using the method of Riera*
  - FE-analysis of building with F-t-Function lumped over impact area
- Since 9/11 the impact of a commercial aircraft came up
- Due to differences within structural setup and dimensions of both plane types and
  due to enhanced capabilities of numerical algorithms the analysis can be performed in one step today

→ integral analysis

**Riera: ‚On the Stress Analysis of Structures subjected to Aircraft Impact Forces', Nuclear Engineering and Design, 1968*

Parameters Passenger Aircraft

Overview
Partners
Tasks
Risk Assessment
Analysis
Conclusion

Classification of commercial passenger aircrafts

I.	Weight > 330 t	e.g. A 380, B 747 and A 340
II.	Weight = 150 - 330 t	e.g. A300 and B767
III.	Weight < 150 t	e.g. A320 and B737

Impact Velocity

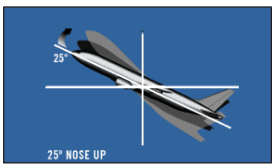
- 70 - 100 m/s (landing) hits close to the ground
- 160 - 175 m/s maximum for hits far from the ground
- defined by national authorities

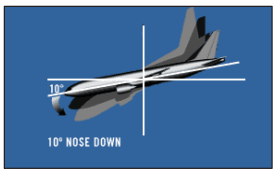
Statistics Air Traffic

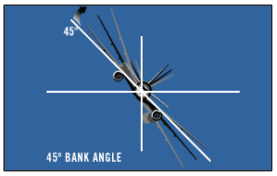
- Statistics about aircraft classes
- Distance to airports (weight reduction)

Flight Parameters

- Angle of impact – aerodynamic stability



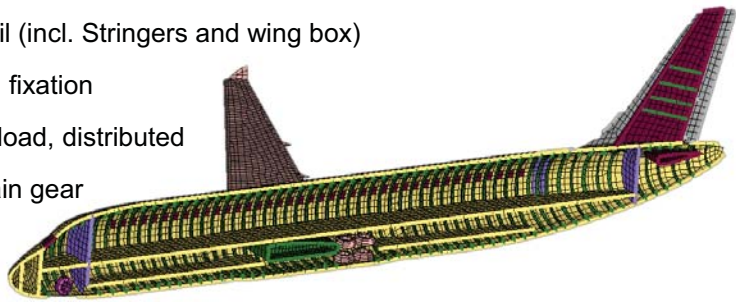




- Topology around building structure
  - pothole
  - obstacles

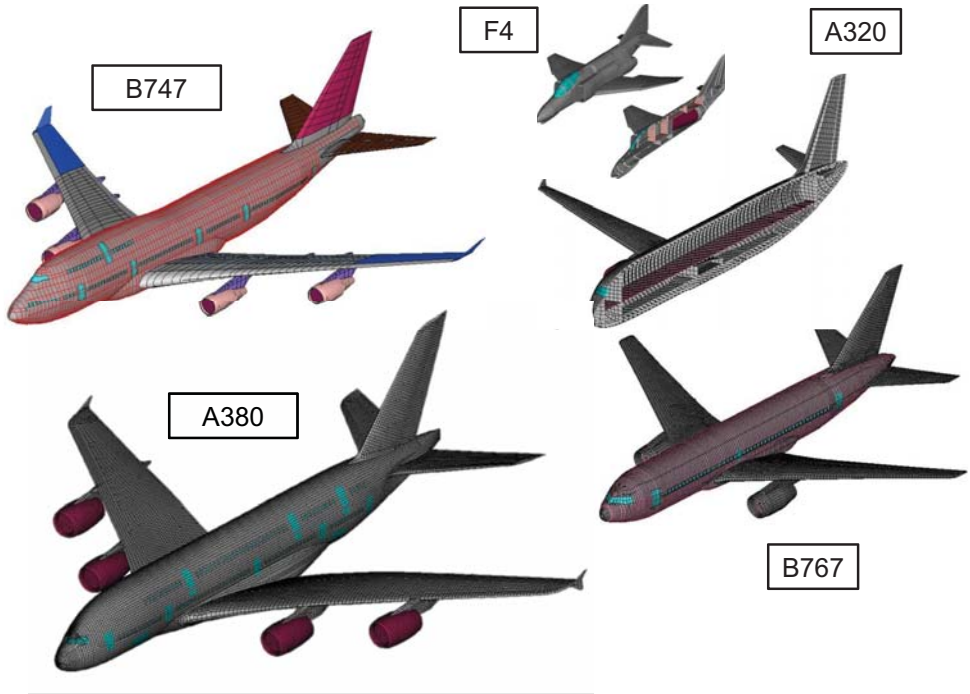
Modelling Setup of Passenger Plane

- Aim of the analysis is assessment of building
- Only the main parts of the aircraft are considered:
  - Fuselage (incl. ribs and stringers),
  - Wings and tail (incl. Stringers and wing box)
  - Turbines with fixation
  - Fuel and payload, distributed
  - Front and main gear



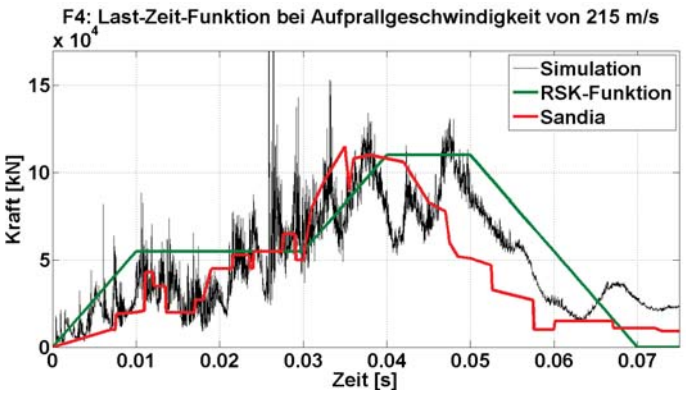
- Material description is nonlinear including plasticity, failure and strain rate dependence

Plane models of Wölfel



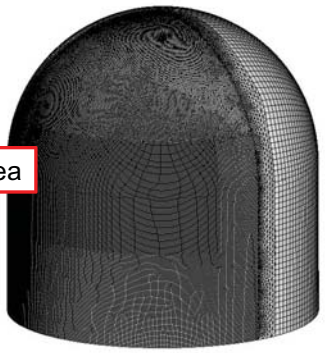
Validation by Sandia Tests F4

- A validation of the simulation procedure by experimental results is for passenger aircraft not possible as no data exist
- A principal validation can be carried out applying the procedure for the crash of the Phantom in comparison to the Sandia Tests

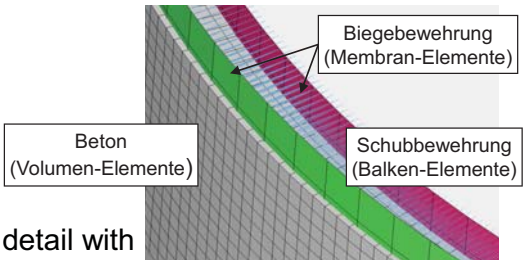


Modelling Setup Building

- The crash analysis is carried out on a exemplary reactor building, without anv soil effects. i.e. structure is fixed at the bottom



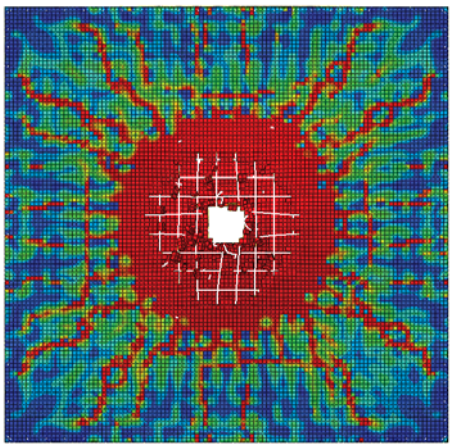
Geometric dimensions:
- height cylinder 30 m
- radius cylinder 15 m
- height Hemisphere 30 m
- wall thickness 1.8 m

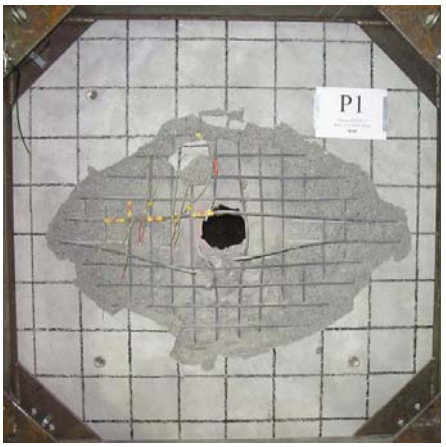


- The wall setup is considered in detail with the concrete, the bending and shear reinforcement
- The material definitions are nonlinear including failure and strain rate dependence: Concrete - Damaged Plasticity Model;
  Reinforcement - Johnson-Cook Plasticity Model

Punching Test: Result Plate

- Validation by VTT Tests within the IRIS-Benchmark 2010/2012
- Shooting a Missile (v = 135 m/s) at a Concrete Plate
- Comparison Test and Simulation via Damage, Displacement



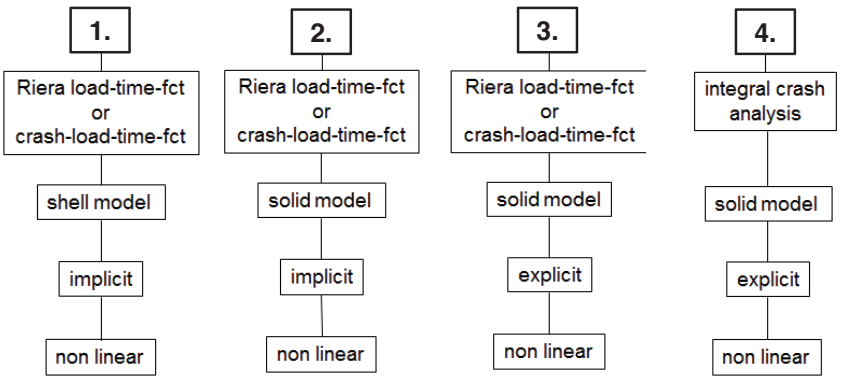


Crash Analysis

- Animation for initial velocity of 160 m/s

Variants of Analyses

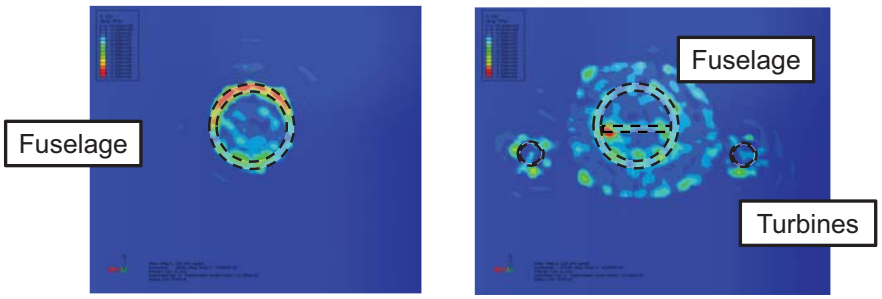
- The capabilities of numerical analysis open up a variety of new techniques



- We shall concentrate at the integral crash analysis.This analysis type is mandatory, if the target is not rigid and plane and structure interact. This is e.g. the case if an obstacle in front of the structure prevents the plane to impact the structure.

First Results of Integral Crash Analysis

- The local load distribution are different
- F-t-approach applies lumped pressure over complete area
- Integral approach has inhomogeneous pressure distribution (depending on the interaction between building and aircraft) – leads to higher local destruction
- Load time functions are not conservative



Compressive stress distribution for integral approach at t=0.025 and 0.08 s

Summary

- According the improved Soft-and Hardwaretechnologies the variety of analyses methods is enhanced by the integral approach.
- With the integral approach a more exact analysis can be done concerning the parameters of the impact (flight angle, partly hitting the structure …)
- With the integral approach the till now divided analyses types local, global and vibration are combined in one run.
- Only with the integral approach non-rigid protection capacities can be investigated.
- We shall develop and use the integral approach in the comming year of this reseach project.

Thank you for your Attention!

RAPID-N: A tool for mapping Natech risk due to earthquakes

Serkan Girgin, Elisabeth Krausmann

DG JRC, EC

email: elisabeth.krausmann@jrc.ec.europa.eu

RAPID-N: A tool for mapping Natech risk due to earthquakes

S. Girgin, E. Krausmann

European Commission, Joint Research Centre
Institute for the Protection and Security of the Citizen
Ispra, Italy

Serving society
Stimulating innovation
Supporting legislation

Definition

A "Natech" accident is a "chemical accident" caused by a natural hazard or a natural disaster.

Chemical accidents include accidental **oil and chemical spills**, **gas releases**, and **fires or explosions** involving hazardous substances from **fixed establishments** (e.g. petrochemical, pharmaceutical, pesticide, storage depot), and **oil and gas pipelines**


Earthquake, Turkey, 1999


Hurricane, USA, 2005


Floods, Czech Republic, 2002


Earthquake, China, 2008

Natural-Event Impact on Chemical Infrastructures

At least 40% of surveyed EU MS and OECD Member Countries have experienced one or more Natech accident, sometimes with fatalities and injuries, environmental or economic damage, or supply disruption

+ Tohoku earthquake and tsunami (Japan, 2011): multiple Natech accidents, 6 refineries halted shutting in 30% of refining capacity, major fires and explosions in 2 refineries;

+ Hurricanes Katrina & Rita (USA, 2005): 113 off-shore platforms destroyed, 163 severely damaged; hike in global oil price; release of 30 million litres oil onshore;

+ Kocaeli earthquake (Turkey, 1999): multiple fires in a refinery producing 1/3 of Turkey's total oil-related output; international assistance required to cope with the accident.

Expected increase of Natech risk due to more hazards (climate change, industrialisation) and higher vulnerability of society (urbanisation, interconnectedness)

Natech Risk-Reduction Situation

- Legislation, codes and standards for chemical-accident prevention rarely address Natech risk explicitly
- There is little knowledge on the dynamics of Natech accidents
- There are hardly any methodologies and tools for Natech risk assessment and no guidance for industry on how to assess Natech risk
- Emergency-response plans do not consider the characteristics of Natech accidents (loss of utilities)
- There are no Natech risk maps to identify areas at risk

. from a JRC survey on the status of Natech risk reduction in the OECD and in EU MS

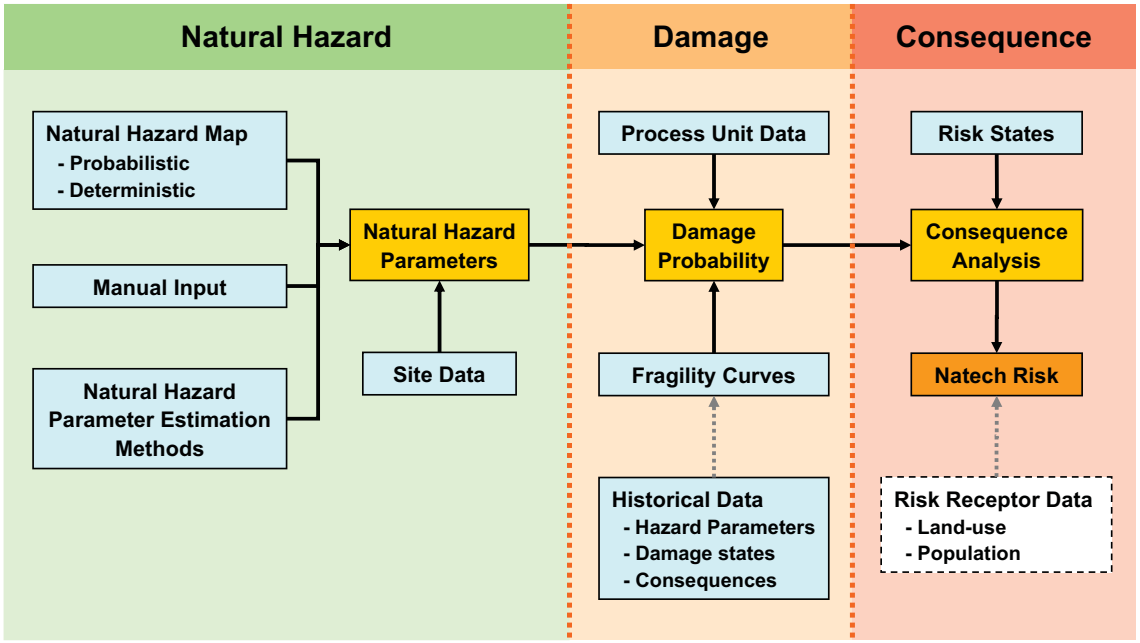
E. Krausmann, D. Baranzini (2012) Natech risk reduction in the European Union, J Risk Research 15(8): 1027-1047

Natech Risk Mapping

- **Natech risk maps are considered a high priority need for:**
  - Identification of Natech prone areas (land-use planning)
  - Emergency-response planning
- **Hardly any Natech risk maps exist in the EU/OECD**
  - **Simple overlay of natural hazards and industrial facilities**
  - **Do not consider site-specific features**
    - Expected release scenarios
    - Existing safety measures

→ Development of a unified Natech risk assessment and mapping methodology and implementation as a software tool

Methodology



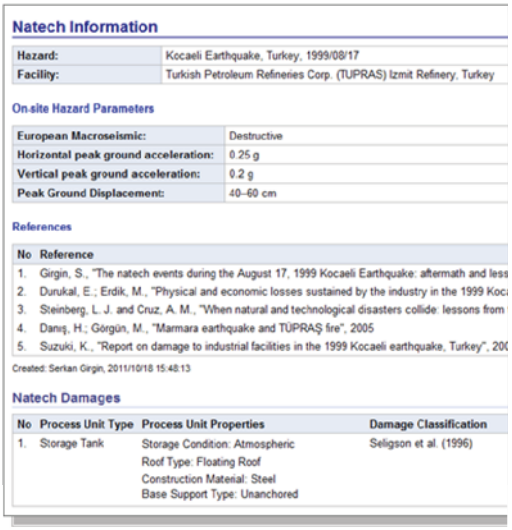
Rapid Natech Risk Mapping Tool: RAPID-N

- Web-based application
  - Multilingual
- Easy and quick data entry
- Rapid analysis and visualization
- No commercial packages

- Modular architecture
  - Scientific Tools
  - Natural Hazards and Natechs
  - Facilities and Process Units
  - Risk Assessment
- Current focus on earthquakes

Natural Hazards and Natechs Module

- Hazards
  - Source parameters
- Earthquake Catalog Data
  - Online monitoring (USGS, EMSC)
  - Automated update of hazard data
- On-site Hazard Data
- Hazard Maps
  - USGS Shakemaps
- Natechs
  - On-site hazard parameters

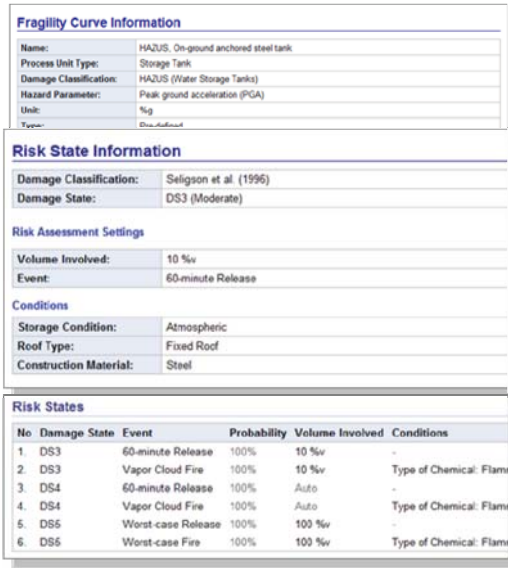


Facilities and Process Units Module

- Facilities
  - Activity, location, operator
  - Site properties
- Substances
  - Identifiers
  - Physico-chemical properties
- Process Units/Groups
  - Process unit characteristics
  - Stored substances
  - Lumped process unit data
- Typical Process Units
  - Process unit data substitute

Risk Assessment Module

- Damage Classifications
  - Set of damage states
- Fragility Curves
  - Damage probability vs. PGA
- Risk States
  - Damage state
  - Damage parameters, e.g.:
    - Natech event (e.g. BLEVE)
    - Conditional probability (e.g. 50%)
    - Volume involved (e.g. 10 %v)
  - Validity conditions
- Consequence modeling



Fragility Curve Information

Name:	HAZUS, On-ground anchored steel tank
Process Unit Type:	Storage Tank
Damage Classification:	HAZUS (Water Storage Tanks)
Hazard Parameter:	Peak ground acceleration (PGA)
Unit:	%g

Risk State Information

Damage Classification:	Seligson et al. (1996)
Damage State:	DS3 (Moderate)

Risk Assessment Settings

Volume Involved:	10 %v
Event:	60-minute Release

Conditions

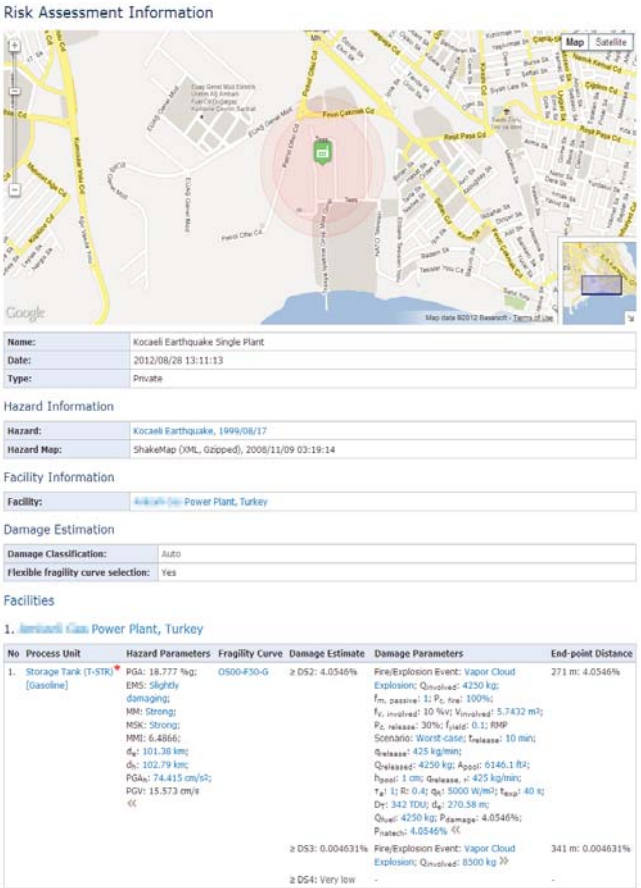
Storage Condition:	Atmospheric
Roof Type:	Fixed Roof
Construction Material:	Steel

Risk States

No	Damage State	Event	Probability	Volume Involved	Conditions
1.	DS3	60-minute Release	100%	10 %v	-
2.	DS3	Vapor Cloud Fire	100%	10 %v	Type of Chemical: Flam
3.	DS4	60-minute Release	100%	Auto	-
4.	DS4	Vapor Cloud Fire	100%	Auto	Type of Chemical: Flam
5.	DS5	Worst-case Release	100%	100 %v	-
6.	DS5	Worst-case Fire	100%	100 %v	Type of Chemical: Flam

Risk Assessment

- Natech damage assessment
  - Calculation of hazard parameters
  - Estimation of damage probability fragility curves
- Natech consequence analysis
  - Estimation of (worst-case) consequence scenarios
  - Calculation of end-point distances using RMP methodology (US EPA)
    - Toxic
    - Flammable
- Output
  - Risk map
  - Summary report



Risk Assessment Information

Name:	Kocaeli Earthquake Single Plant
Date:	2012/08/28 13:11:13
Type:	Private

Hazard Information

Hazard:	Kocaeli Earthquake, 1999/08/17
Hazard Map:	ShakeMap (XML, Gzipped), 2006/11/09 03:19:14

Facility Information

Facility:	[redacted] Power Plant, Turkey

Damage Estimation

Damage Classification:	Auto
Flexible fragility curve selection:	Yes

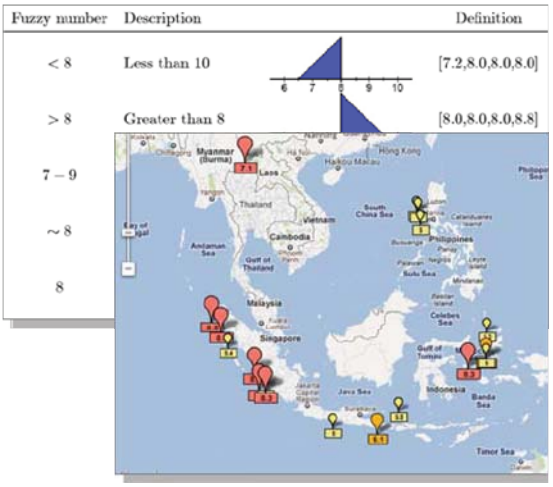
Facilities

1. [redacted] Power Plant, Turkey

No	Process Unit	Hazard Parameters	Fragility Curve	Damage Estimate	Damage Parameters	End-point Distance
1.	Storage Tank (T-STR) [Gasoline]	PGA: 18.777 %g; EMS: Slightly damaging; MM: Strong; MSK: Strong; MMI: 6.4866; d_e: 101.38 km; d_h: 102.79 km; PGA_h: 74.415 cm/s²; PGV: 15.573 cm/s	OS00-FS0-G	≥ DS2: 4.0546%	Fire/Explosion Event: Vapor Cloud Explosion; $Q_{involved}$: 4250 kg; $f_{m,\ passive}$: 1; $P_{c,\ fire}$: 100%; $f_{V,\ involved}$: 10 %v; $V_{involved}$: 5.7432 m³; $P_{c,\ release}$: 30%; f_{yield}: 0.1; RMP Scenario: Worst-case; $t_{release}$: 10 min; $q_{release}$: 425 kg/min; $Q_{released}$: 4250 kg; A_{pool}: 6146.1 ft²; h_{pool}: 1 cm; $q_{release,\ v}$: 425 kg/min; τ_a: 1; R: 0.4; q_h: 5000 W/m²; t_{exp}: 40 s; D*: 342 TDU; d_e: 270.58 m; Q_{fuel}: 4250 kg; P_{damage}: 4.0546%; P_{natech}: 4.0546%	271 m: 4.0546%
				≥ DS3: 0.004631%	Fire/Explosion Event: Vapor Cloud Explosion; $Q_{involved}$: 8500 kg	341 m: 0.004631%
				≥ DS4: Very low	-	-

Scientific Tools Module

- Statistics and curve-fitting
- Fuzzy arithmetic
- Automated unit conversion
- Mapping
  - Google Maps
  - GIS analysis library



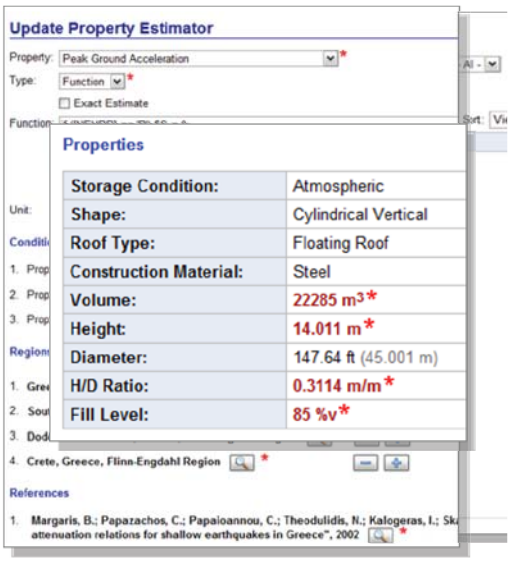
Property Estimation Framework

- Minimize data requirement
- Increase flexibility
  - No hard-coded functions

Support module

Property Estimation Framework

- Generic framework
  - Natural hazard properties (e.g. PGA)
  - Site properties (e.g. Soil class)
  - Process unit properties (e.g. Volume)
  - Substance properties (e.g. Density)
  - Facility properties
- Fixed value or complex function
- Location-aware
- Automatic selection of "most suitable"
  - Recursive
  - Exhaustive



Summary

- RAPID-N features a web-based, integrated framework for Natech risk assessment and mapping (for earthquakes)
- **RAPID-N allows rapid assessment of natech risks with minimum data input**
- Application areas:
  - **Land-use planning**
  - **Emergency planning**
  - **Preliminary Natech damage estimation**
- Current status:
  - **Release phase (expert validation)**
  - **Included data (from open sources)**
    - **> 18,500 earthquakes**
    - **> 7,300 earthquake maps**
    - **> 5,500 industrial facilities (only for internal use)**

Future Work

- Automated Natech damage and consequence estimation (Alert)
  - E.g. Automatic warning of authorities by the JRC
- Consideration of risk receptors (population)
- Extension to other natural hazards
  - Floods
- Extension to other industrial facilities
  - Pipelines

Development of a Risk Assessment and Resilience analysis platform by the JRC

Georgios Giannopoulos, Bogdan Dorneanu, Olaf Jonkeren,

DG JRC, EC

email: georgios.giannopoulos@jrc.ec.europa.eu

A GIS-based federated platform for resilience and risk assessment of critical infrastructure networks

Georgios Giannopoulos, Bogdan Dorneanu, Olaf Jonkeren*

Joint Research Centre
Security Technology Assessment Unit

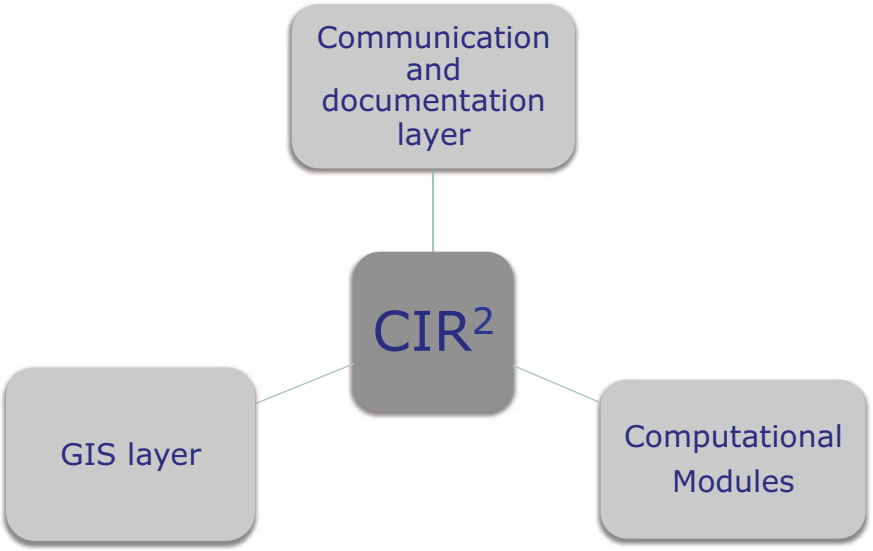
www.jrc.ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation

A platform for harmonized risk and resilience assessment of CIs: CIR²

High Level Objectives	Propose a platform for harmonized **risk** and **resilience** assessment of critical infrastructures at **regional**, **national** or **international** level
	Assess infrastructures at **asset** and/or at **systems** level
	Establish a community of **researchers** and **policy makers** that can **exchange information**, **simulations** and **best practices** in a harmonized and consistent way
	Respond to the **high level requirements** of the EPCIP policy on **prevention**, **preparedness** and **response**

Structure



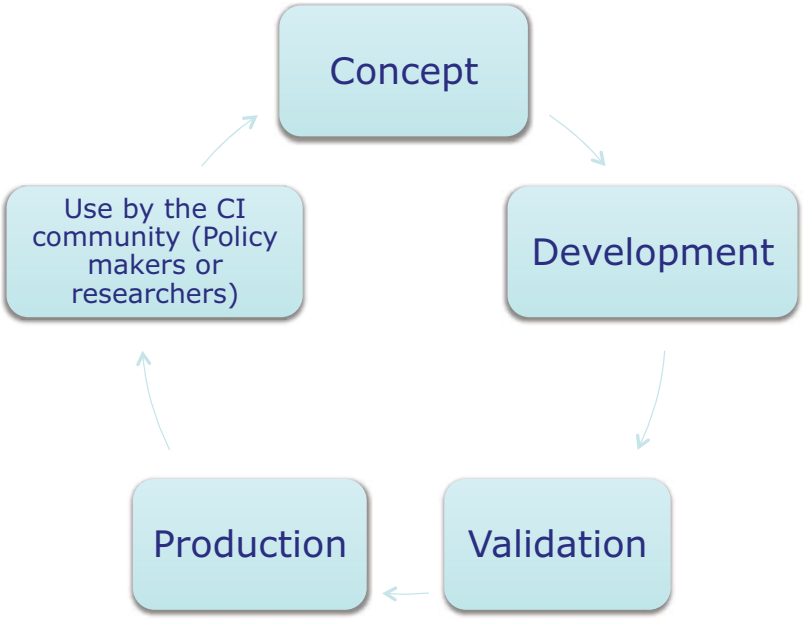
What do we want to offer?

A system that can be both available **online** or as **standalone** version but with **federation** capabilities

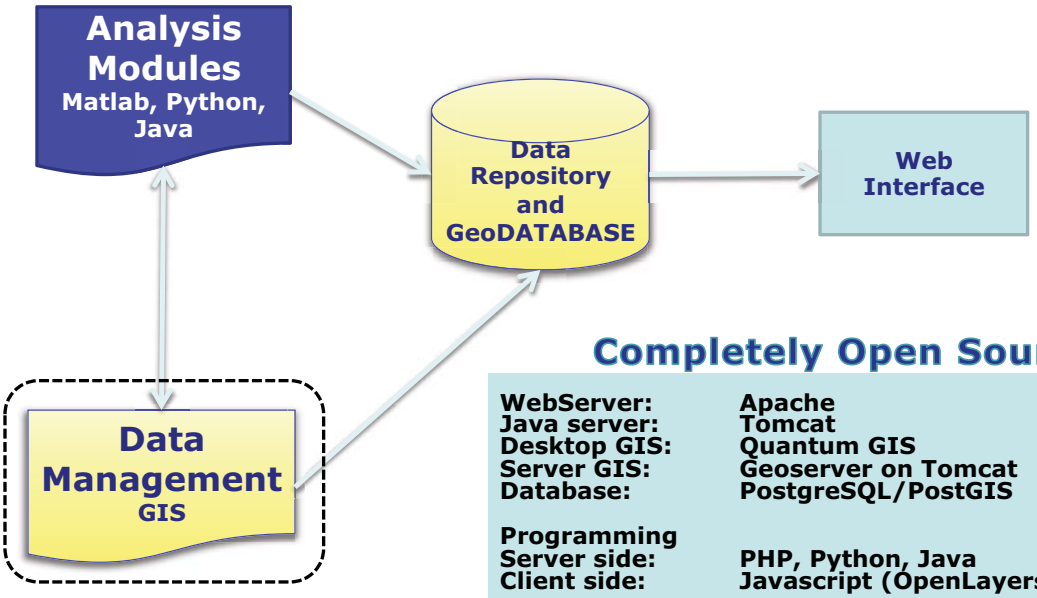
Seamless federation of different models over a common infrastructure

Both a **research tool** for model validation as well as a **production** tool that can be used for CI **risk** and **resilience** assessment

A comprehensive platform for model development



GIS Platform – Technology Overview



Completely Open Source

WebServer:	**Apache**
Java server:	**Tomcat**
Desktop GIS:	**Quantum GIS**
Server GIS:	**Geoserver on Tomcat**
Database:	**PostgreSQL/PostGIS**
Programming	
Server side:	**PHP, Python, Java**
Client side:	**Javascript (OpenLayers, GetExt)**

Data input: Several possibilities

Using data stored in an existing database

- Geospatial information for selected infrastructure can be **stored** in the system
- The user may decide which part of the data to use
- **Authentication** required (In principle very limited data will be stored in the system)

Uploading data remotely into an existing database

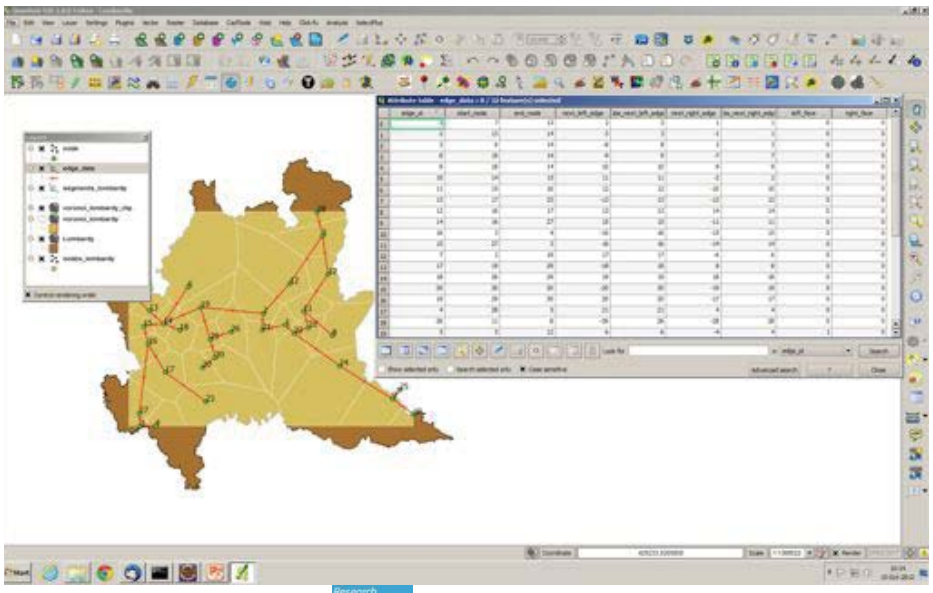
- Data will be **uploaded** to the system database for the processing stage using a file (most common GIS Formats)

Creating data for the processing "online"

- Data will be **digitized** using the web interface and then passed to the processing modules **without storing** them in any database

Access to an existing database: local or external

Access to the existing database: Selection of a subset

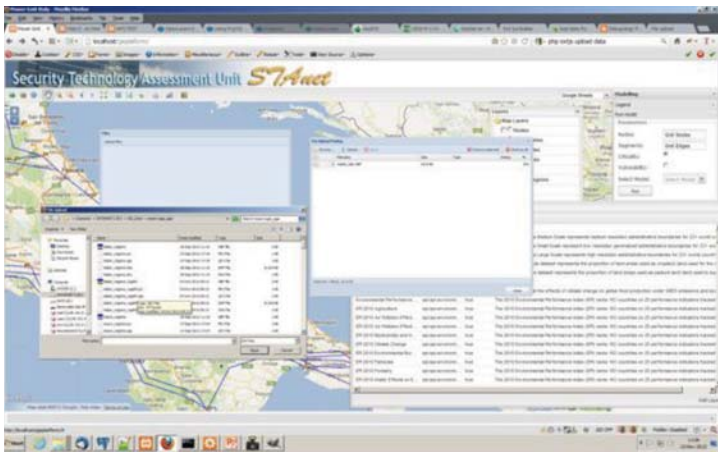


GIS file upload

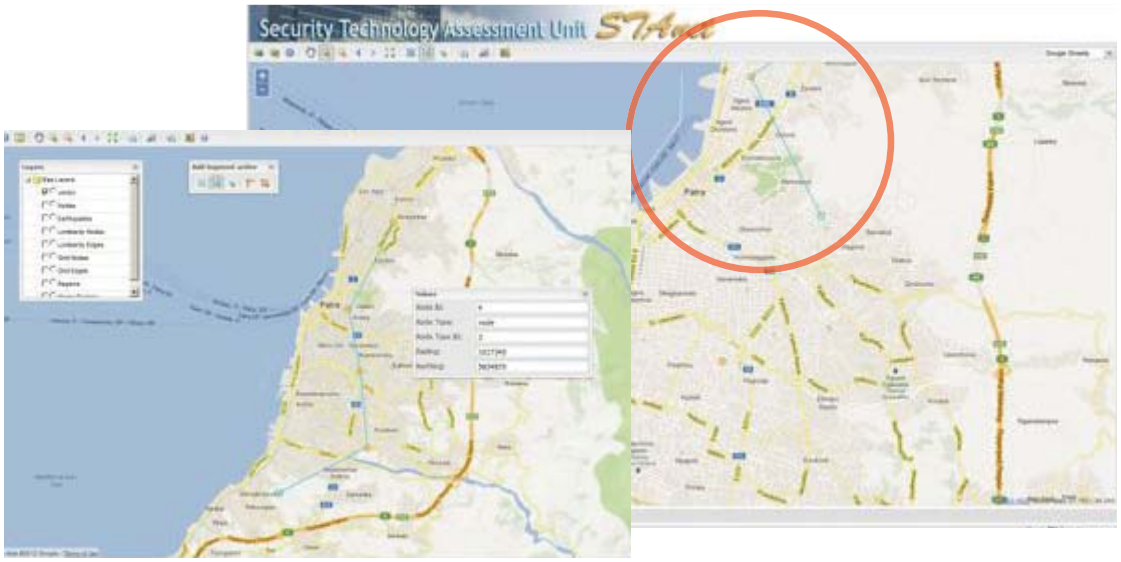
The user may upload his/her own GIS file

Perform assessments using this data and the modules that will be plugged-in to the system

Save the data into the **database** to make it available to the other users or just **delete** them



Digitize the grid using maps/satellite images "on-the-fly"



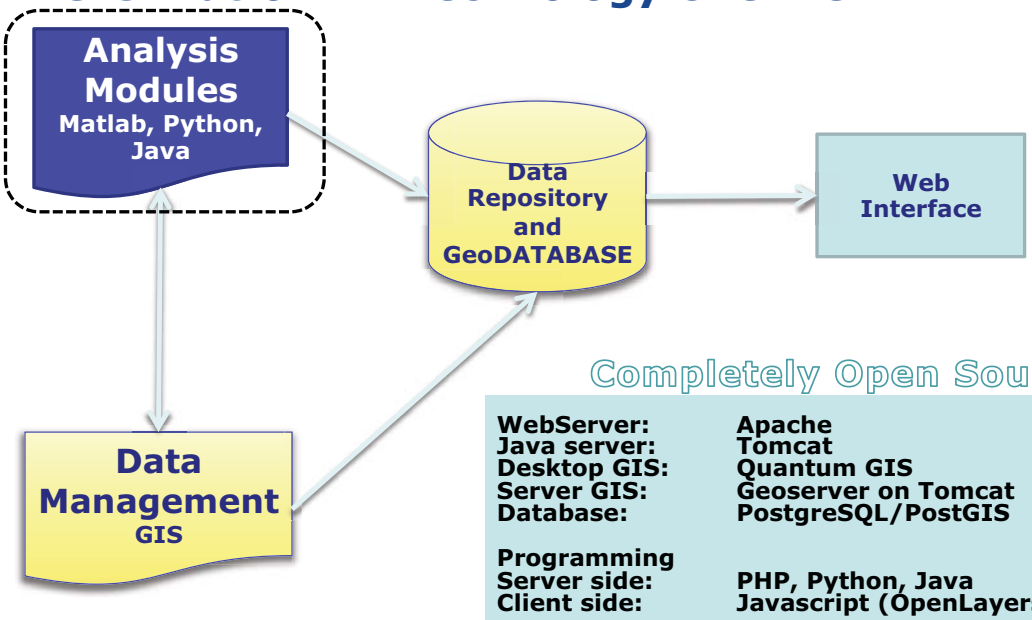
Online processing

Visualize **networked infrastructures** for which there is **no available database**

Create additional **dependencies** layers (e.g. functional) between elements of different networked infrastructures for which databases already exist (**stored or uploaded**)

Enabling emergency management: Possibility to **modify** the links between **assets and infrastructures** "on the fly" and according to the evolution of an emergency.

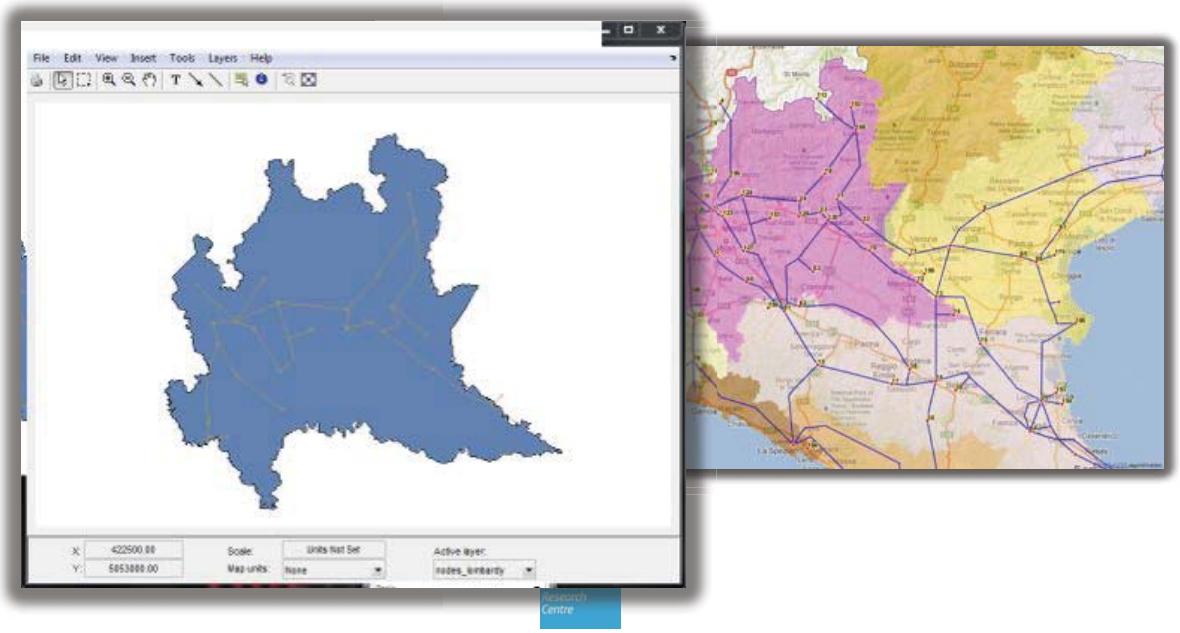
GIS Platform – Technology Overview



Completely Open Source

WebServer:	**Apache**
Java server:	**Tomcat**
Desktop GIS:	**Quantum GIS**
Server GIS:	**Geoserver on Tomcat**
Database:	**PostgreSQL/PostGIS**
Programming	
Server side:	**PHP, Python, Java**
Client side:	**Javascript (OpenLayers, GetExt)**

Example of MATLAB / GIS federation

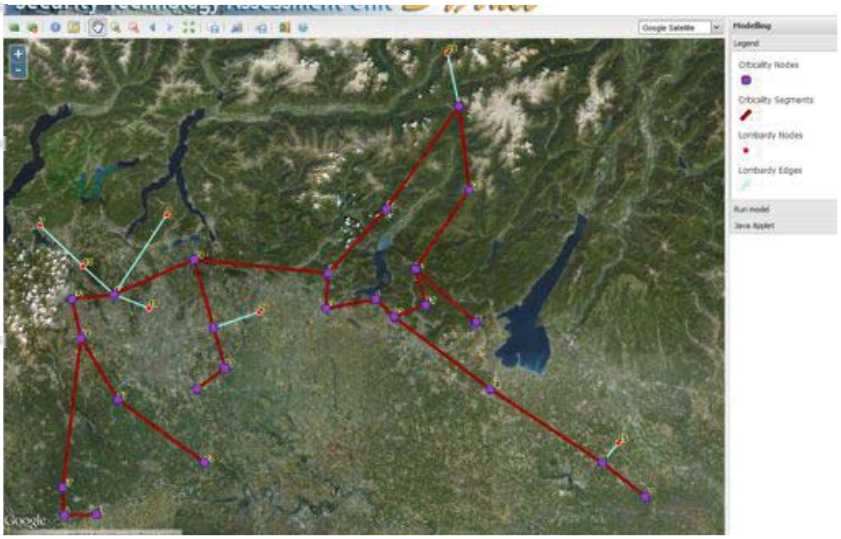


Example of MATLAB / GIS federation

Criticality analysis

A module has been developed in Matlab and has been plugged-in to the system

Evaluation of all nodes affected by a node disruption

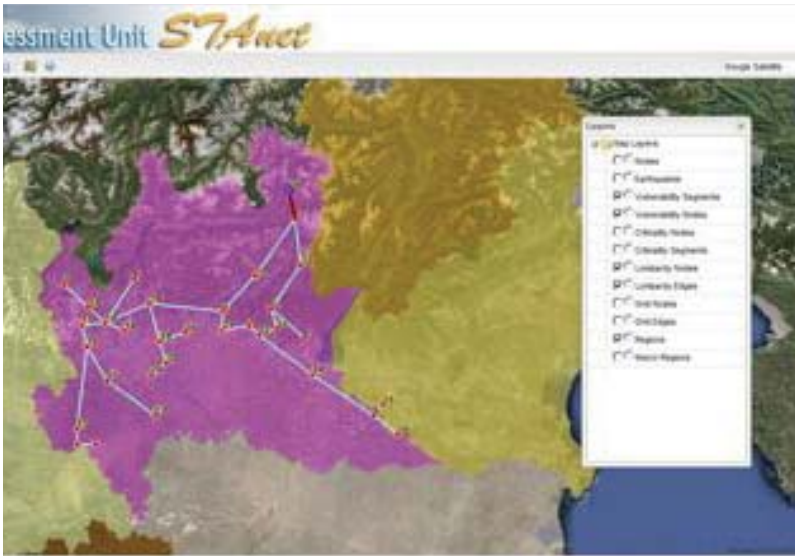


Example of MATLAB / GIS federation

Vulnerability analysis

A module has been developed in Matlab and has been plugged-in to the system

Evaluation of all nodes that may affect the operation of one node



Communication layer

Federation at communication layer

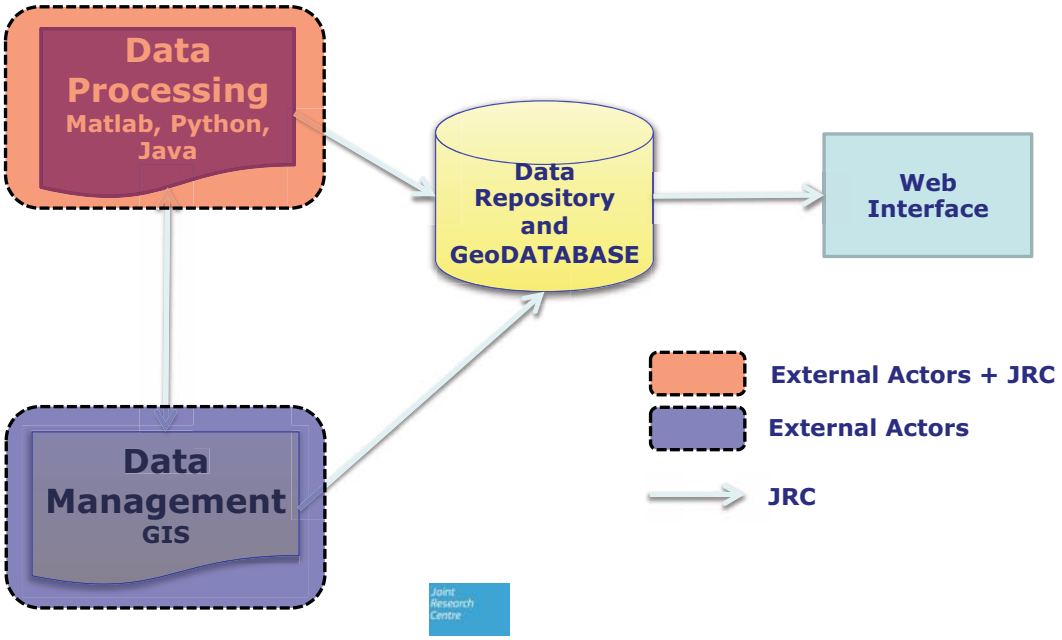
Exchange of **analyses**, **information**, **data** etc. on the basis of a common platform

Possibility to post **requests for analyses** that may be undertaken by the research community

Possibility to **upload documents** and other scientific material linked to an **asset**, an **infrastructure** or a **region** and make it available to the rest of the community

Associate **incident reports** and other **documentation** to **assets** and **infrastructures**

The future: Collaborative development - roles



Collaborative development

- Input from **policy makers** on the **analysis needs**
- Input to the scientific community to develop the necessary **modules** and **analysis tools**
- JRC facilitates the **interface** and **interoperability** of modules as well as the **development** of certain **analysis modules**.
- Developed so far:
  - **Structural analysis of networks**
    - Criticality of nodes
    - Vulnerability of nodes
    - Clustering coefficients
    - Minimum path
    - Reconfiguration of networks due to disruption on the basis of structural characteristics
  - **Systems engineering - dependencies and interdependencies**
  - **Economic impact of CI disruption using I/O modeling**

Critical Infrastructure Resilience Assessment The Systems Engineering Component

Bogdan Dorneanu, Roberto Filippini, Olaf Jonkeren, Georgios Giannopoulos*

Joint Research Centre
Security Technology Assessment Unit

www.jrc.ec.europa.eu

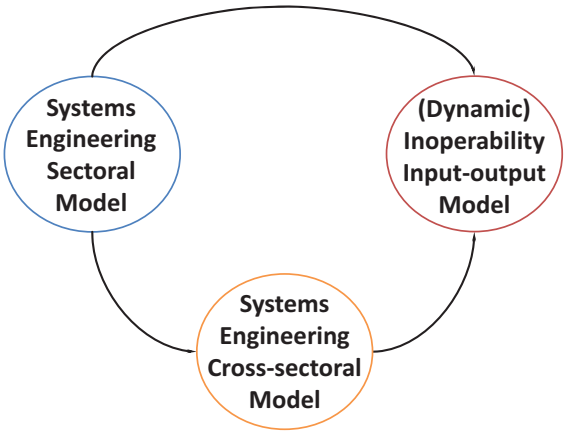
Serving society
Stimulating innovation
Supporting legislation

Outline

- Methodology
- Systems Engineering model (SEM)
- Model implementation
- Future work

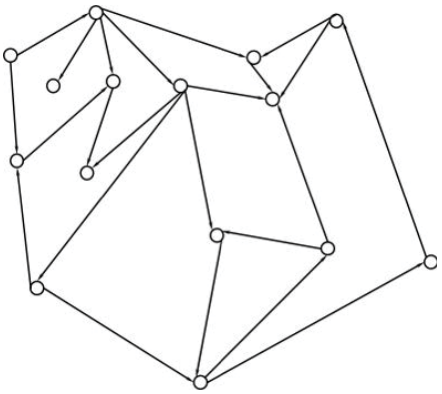
Methodology

- Combined ***systems*** **engineering -** economic inoperability input-output model (SE- (D)IIM)
  - *SEM*
    - Analysis of system's performance degradation and/or recovery
    - Single Critical Infrastructure
    - Cross-sector Critical Infrastructures
  - *(D)IIM*
    - Estimates economic losses resulting from absence of resources



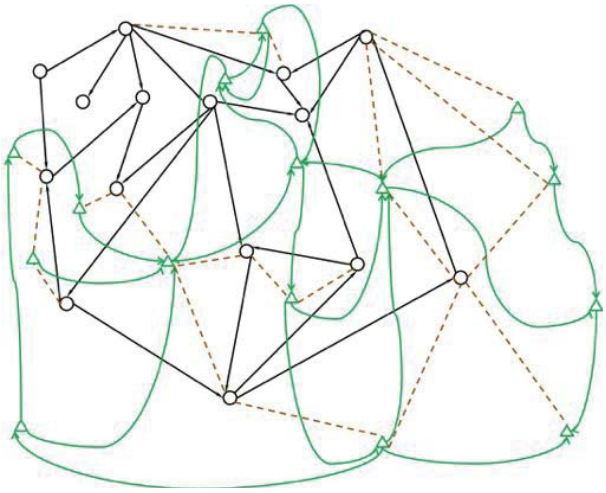
Systems Engineering model (SEM)

- Automatic extraction of network topology (geo referenced) from the GIS (single or multiple CI)



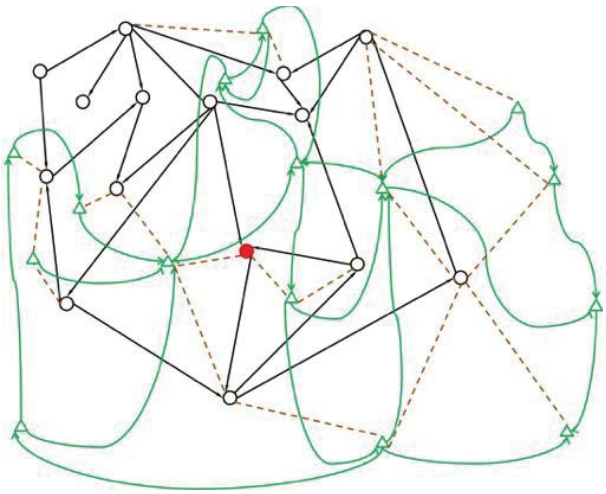
Systems Engineering model (SEM)

- Automatic extraction of network topology (geo referenced) from the GIS
- Assignment of the network functional dependencies
- Model parameters
  - Buffering time
  - Recovery time
  - Network reconfiguration
  - …



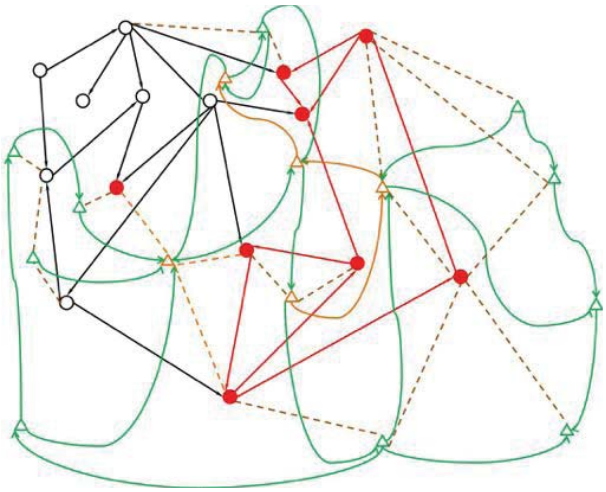
Systems Engineering model (SEM)

- Injection of the disturbance in one or more nodes



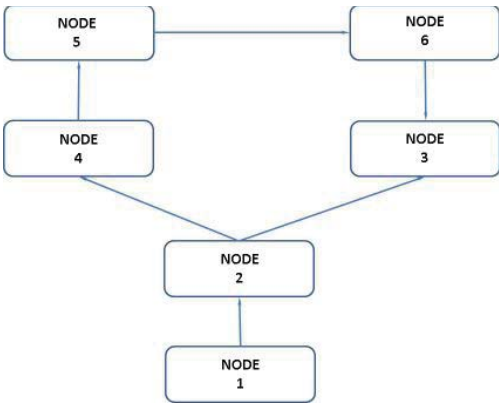
Systems Engineering model (SEM)

- Injection of the disturbance in one or more nodes
- Result – perturbation propagation determined by the (inter)dependencies among the network nodes



Systems Engineering model (SEM)

- Cross-sector CI's
- Higher level of abstraction

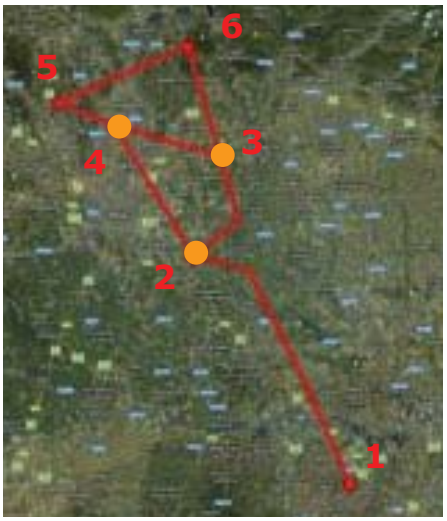


Systems Engineering model (SEM)

- **Cross-sector CI's**
  - A disturbance affects a particular node and propagates

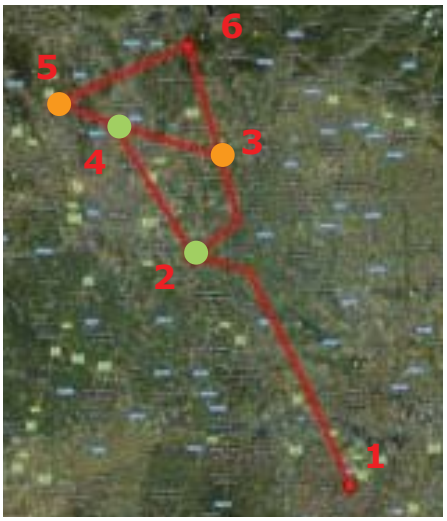
Systems Engineering model (SEM)

- **Cross-sector CI's**
  - A disturbance affects a particular node and propagates
  - Each node may fail after a time to failure



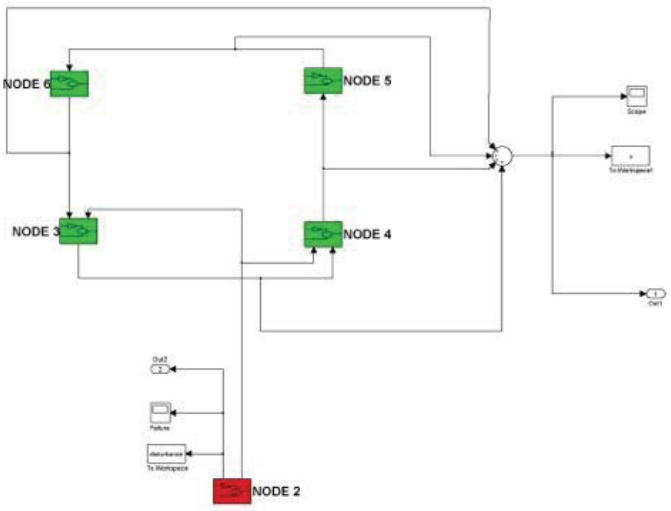
Systems Engineering model (SEM)

- **Cross-sector CI's**
  - A disturbance affects a particular node and propagates
  - Each node may fail after a time to failure
  - Each node may recover after a time to recovery

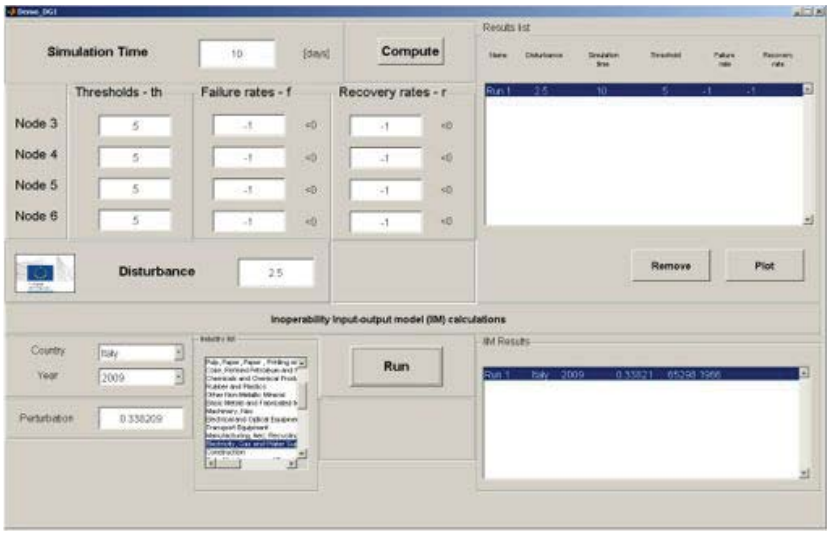


Model implementation in Simulink

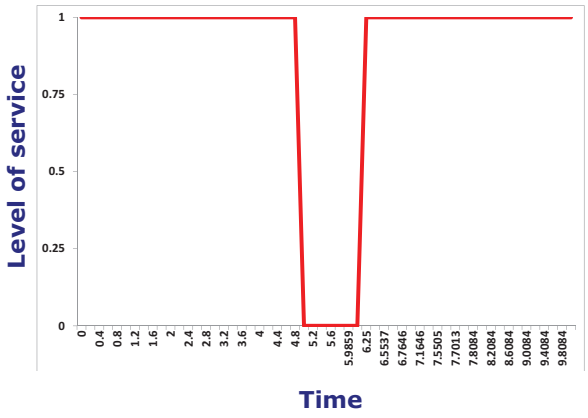
- Automatic model building using the GIS topology
- Model parameters inserted through the GIS
- Two types of nodes
  - Directly affected node
  - Dependent node

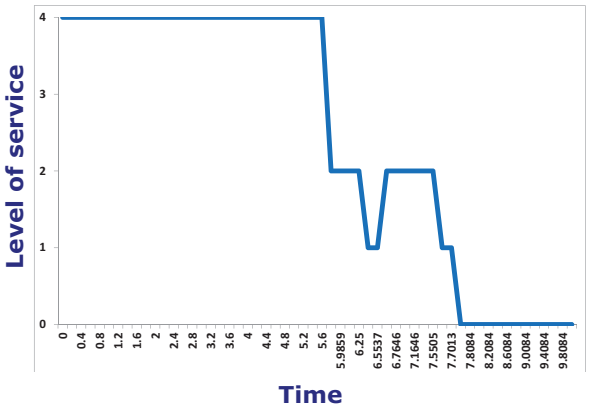


Model implementation



Model implementation

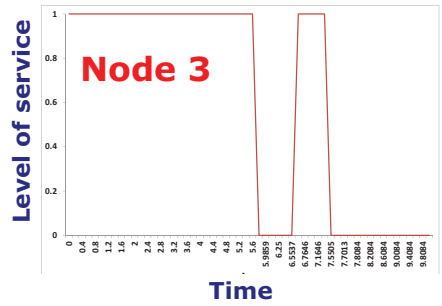


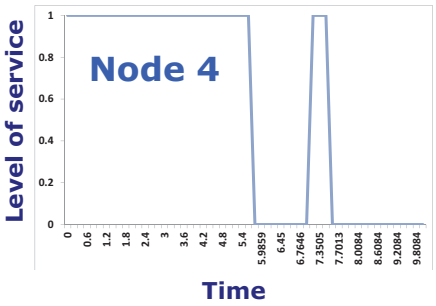


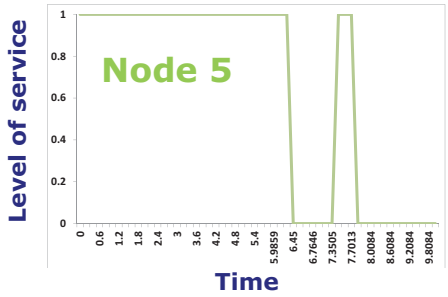
Disturbance of NODE 2

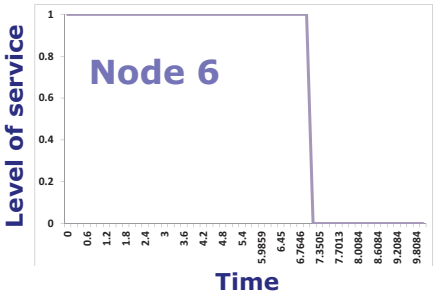
Network response

Model implementation

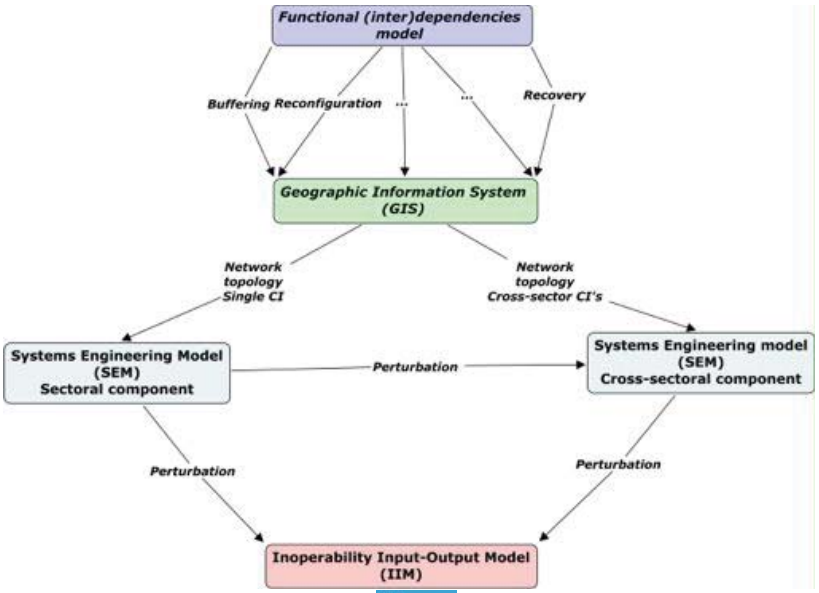








Summary SEM



Future work

- Modelling network's behavior using a dynamic inoperability input-output approach
- Development of node behavior library of models for failure and recovery rates based on
  - Network type
  - Threat type
- Introduction of model parameters through GIS layer
- Interoperability with GIS layer in order to recognize the type of data required and adapt the input fields accordingly

Critical Infrastructure resilience assessment
The economic component

Olaf Jonkeren, Bogdan Dorneanu, Georgios Giannopoulos*

Joint Research Centre
Security Technology Assessment Unit

www.jrc.ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation

Model

Goal: estimate economic losses following from infrastructure failure

Requirements model:

- 27 EU countries
- Economic resilience
- Focus on CI's and KRSC's
- Input from SE model
- Treat 'workforce' as a CI
- All infrastructure approach
- All hazards approach
- Include indirect effects/ interdependencies

The basis: Input-Output model

- Impact assessment method
  Aims to map out the direct and indirect consequences of an initial impulse into an economic system across all economic sectors.
- Depicts the system-wide effects of an exogenous change in a relevant economic system.
- Output measured in terms of economic losses: value (€) of lost production.

The basis: Input-Output model

		PRODUCERS AS CONSUMERS								FINAL DEMAND			
		Agric.	Mining	Const.	Manuf.	Trade	Transp.	Services	Other	Personal Consumption Expenditures	Gross Private Domestic Investment	Govt. Purchases of Goods & Services	Net Exports of Goods & Services
PRODUCERS	Agriculture												
	Mining												
	Construction												
	Manufacturing												
	Trade												
	Transportation												
	Services												
	Other Industry												
VALUE ADDED	Employees	Employee compensation								GROSS DOMESTIC PRODUCT			
	Business Owners and Capital	Profit-type income and capital consumption allowances											
	Government	Indirect business taxes											

Input-Output transactions table

The basis: Input-Output model

Model transformed into an **Inoperability Input-Output model (IIM)**.

Inoperability:
- degree of disfunction of an industry/CI (0-1)
- the level of inability of an industry/CI to perform its intended functions

Two steps:
1 Model estimates how an initial failure spreads in an economic system (a system of CI's and KRSC's).
2 Degree of failure translated in economic losses.

Interoperability Input – Output Model

Inputs needed (simple example):

- Size initial inoperability in directly affected infrastructure (from technological model)

$$q_0 = \begin{bmatrix} 0 \\ 0.15 \end{bmatrix}$$

- Matrix with interdependencies

$$A^* = \begin{bmatrix} 0.15 & 0.5 \\ 0.1 & 0.05 \end{bmatrix}$$

- Column with industrial output

$$x = \begin{bmatrix} 1000 \\ 1500 \end{bmatrix}$$

Interoperability Input – Output Model

Outputs (simple example):

- Inoperability levels

$$q = \begin{bmatrix} 0.099 \\ 0.168 \end{bmatrix} \quad \text{vs.} \quad q_0 = \begin{bmatrix} 0 \\ 0.15 \end{bmatrix}$$

- Economic losses

$$xloss = \begin{bmatrix} 99 \\ 252 \end{bmatrix}$$

Economic Resilience

IIM extended with resilience aspects to make it dynamic (DIIM).

Economic resilience: 'the ability of a CI or system of CI's to mute losses'.

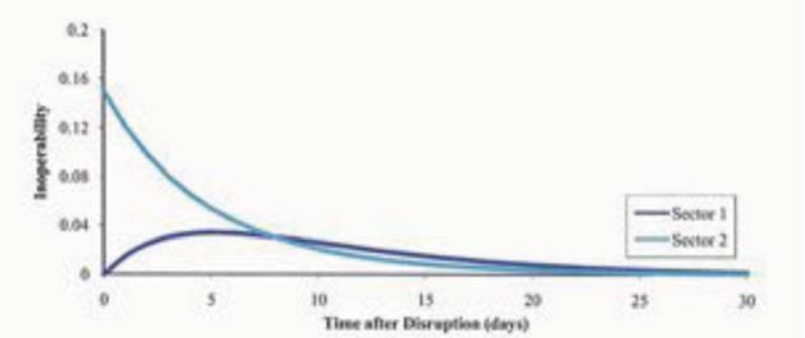
Two types of economic resilience:

- Restorative resilience: speed of recovery of industries after event.
- Absorptive resilience: ability of a CI to mute inoperability following a disruptive event.

Economic Resilience

Restorative resilience

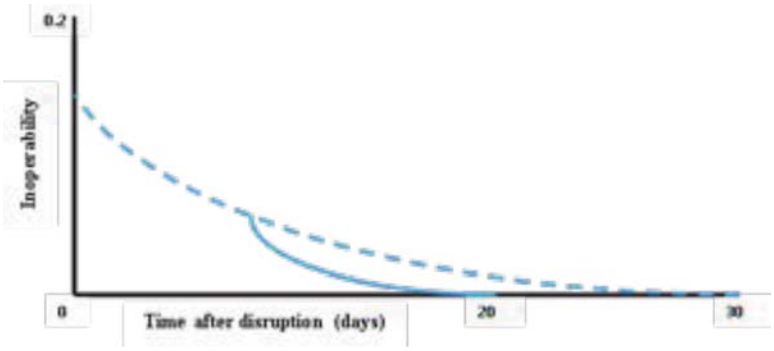
Makes the model dynamic because evolution of inoperability and economic losses over time are modeled.



Economic Resilience

Restorative resilience

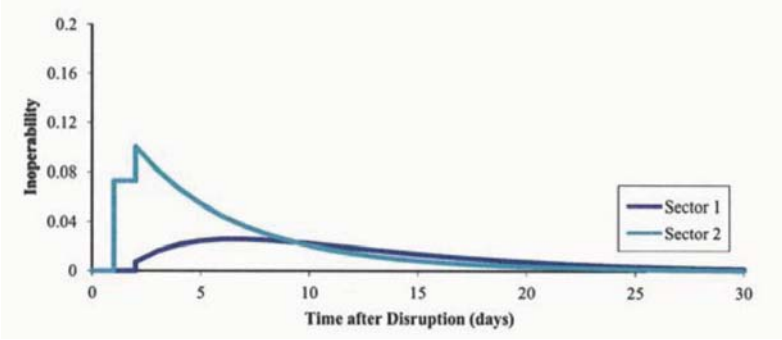
Because speed of recovery may increase (or decrease) during recovery period.



Economic Resilience

Absorptive resilience

Enables the model to analyse effect of preparedness initiatives (presence of inventory, redundancies e.g.)



Data

Source for I-O data: World Input-Output Database (WIOD)
http://www.wiod.org/

- National data on annual economic output
- National data on interdependencies
- 27 EU countries
- 35 industries (including CI's and KRSC's)

Data

CI's and KRSC's included:

Critical Infrastructure /Supply Chain industry
Electricity
Gas
Water
Road
Rail
Pipeline
Inland waterways
Maritime transport
Air transport
Finance
Health
Workforce
Food, beverages, tobacco
Automotive
Wholesale trade
Retail trade

Regional analysis

Data discussed: for economic loss analyses on national level.
What about the regional level?

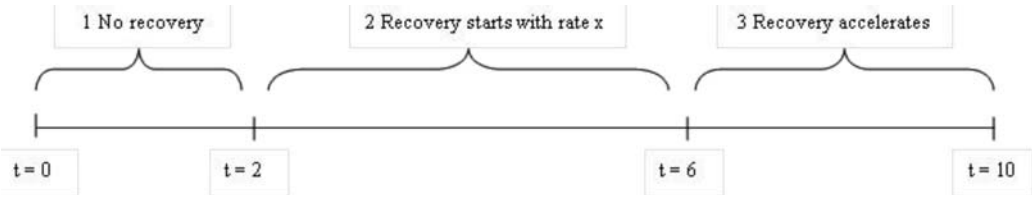
Using national and regional employment data > economic outputs and interdependencies can be estimated for the regional level > facilitates economic loss analyses on regional level.

Relevance:

- Knowledge on economic loss distribution within a country
- More detailed GIS representation
- Facilitates analyses for cross-border regions

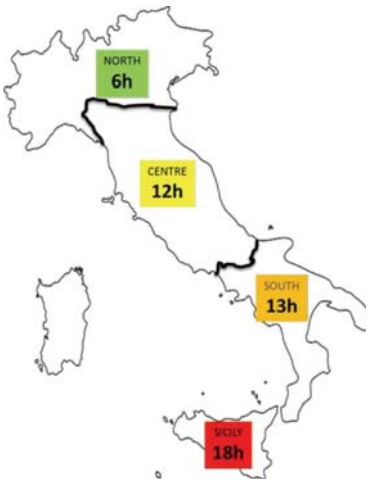
Future work

- Allow existence of a non-recovery period in post-disaster phase

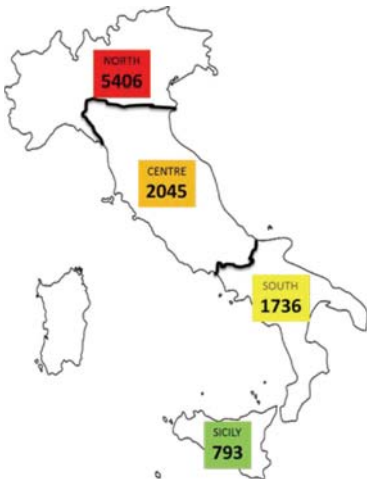


- Allow interdependencies to change over time (inter-industry resilience). Disequilibrium > changes in A* matrix.
- Perform probabilistic analyses > output is a range of economic losses instead of a point estimate.

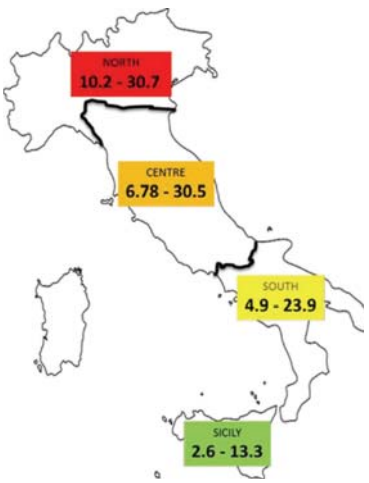
Application of model: Italian CI failure



CI outage time



Regional 1 day economic output (M€)



Regional 1 day economic loss (M€)

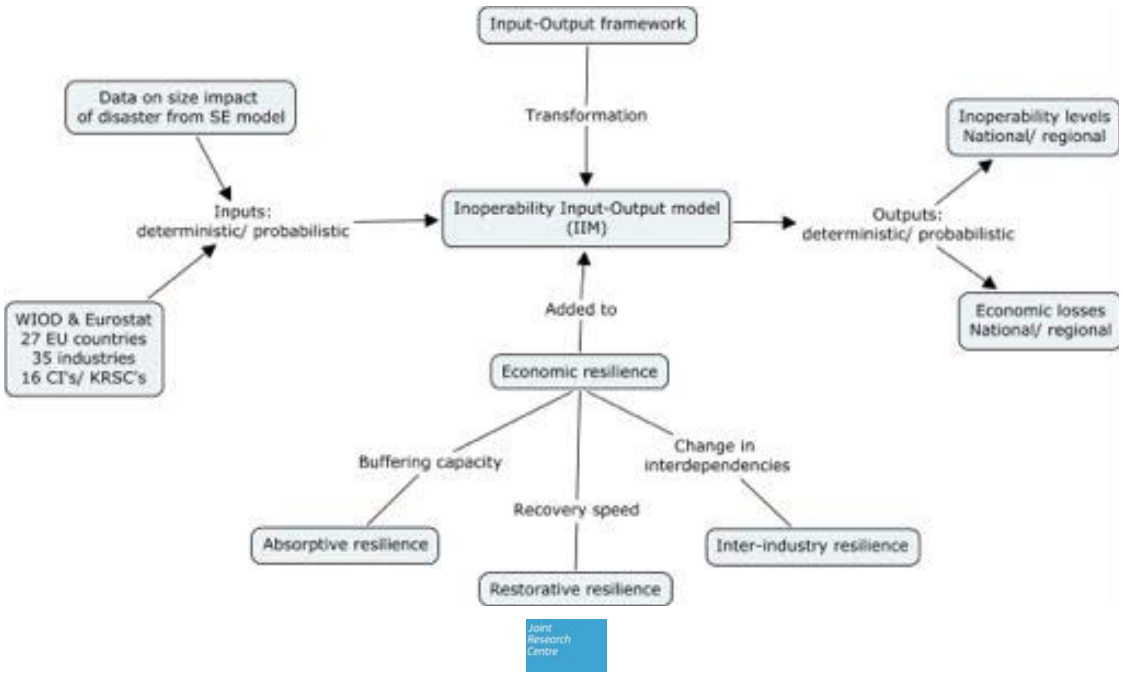
Application of model: Italian CI failure

Comparison Static IIM – Dynamic IIM results

Economic losses (million €) for 11 CI industries only

Model	Industry	Italy	North	Centre	South	Sicily
IIM	1-11	58.90	18.34	18.45	14.51	7.60
DIIM	1-11	16.07	7.13	4.29	3.06	1.59

Summary economic model



European Commission
EUR 25747 EN – Joint Research Centre – Institute for Protection and Security of the Citizen

Title: **CIPS II workshop on research projects financed under the CIPS specific programme**

Authors: Georgios Giannopoulos

Luxembourg: Publications Office of the European Union

2012 – 193 pp. – 21.0 x 29.7 cm

EUR - Scientific and Technical Research series – ISSN 1831-9424
ISBN – 978-92-79-28183-9

doi:10.2788/79113

Abstract

The CIPS projects are financed by DG HOME within the framework of the specific programme «Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks». JRC-IPSC organizes for a second time a dedicated workshop for these projects. The audience of this workshop is composed from researchers, policy makers and national authorities. Bringing together these competences is of instrumental importance in order to steer research projects towards policy makers needs and provide to the policy makers the latest research trends in the domain of Critical Infrastructure Protection.

LB-NA-25747-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

ISBN 978-92-79-28183-9

9 789279 281839